
Mit Stellenmarkt
iX
Anzeige
+++ Große Einführungsaktion! +++
NEU!
Jetzt mit Quad-Core Power!
www.strato.de
siehe Seiten 4 + 5
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK
9 September 2008
€ 5,50
H 10554
September 2008
www.ix.de
iX Magazin für professionelle Informationstechnik
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
Heise
Myspace, StudiVZ, Xing et al.:
Social Networks
Programmierung mit Opensocial-API, Sicherheit
Vorlauf fürs WWW:
25 Jahre BTX
Flash on board:
Acrobat 9
Fibre Channel:
Troubleshooting
Marktübersicht:
Unified Communication
Gesetzeskonform und technisch vorn:
Integrierte Archivsysteme
Embedded-Systeme:
Sicherheitslücken durch Seitenkanalangriffe
Virtualisierer auf dem Mac:
Parallels' Server
Tutorial:
Silverlight
Debugging, Expression Blend
Vergleichstest Peer-to-Peer-Netze:
Anonyme Internetnutzung
4 199148 505501 09

Liebe Grafikkarte!

Wir sind nun schon viele Jahre zusammen. Seit der Zeit, als Du die ersten Punkte auf meinen Bildschirm gemalt hast – damals noch grün auf schwarz –, ist viel geschehen. Du hast Farbe bekommen, mehrmals den Namen geändert – bist Du eigentlich eine geborene Hercules oder CGA? –, mit Lineal und Zirkel umzugehen gelernt, Dich mit perspektivischem Zeichnen vertraut gemacht. Zuletzt hast Du Dir den Künstlernamen GPU (Graphics Processing Unit) zugelegt, weil Du täuschend echt aussehende Bilder von Objekten aus dem Nichts erschaffen, manipulieren und wieder zerstören kannst, und das viele Male pro Sekunde.

Aber Du hast Dich verändert, und nicht zu Deinem Vorteil. Zu Anfang warst Du so schüchtern, dass Du kein Wort gesagt hast. Später hast Du mir leise ins Ohr gesäuselt. Mit der Zeit wurde daraus ein schrilles Kreischen, das meine Nerven über Gebühr strapaziert.

Noch dazu entwickelst Du einen Appetit, der kaum mehr zu stillen ist. Man muss Dich schon intravenös ernähren.

Obendrein hast Du ganz schön zugenommen. Und ständig brauchst Du neue Treiber, weil die alten nicht mehr passen. Natürlich dürfen es nur die von A&N[1] sein – biete ich Dir etwas anderes an, womöglich sogar Open Source, wirst Du zickig. Lässt die Verarbeitungsqualität der Ware mal zu wünschen übrig, gibst Du keine Ruhe, bis ich sie gegen neue umgetauscht habe.

Anfangs war ich noch begeistert, als Du Deine Schwester Crossfire-SLI[2] eingeladen hast, bei uns zu wohnen. Aber Ihr sitzt ständig nur zusammen und tuschelt hinter meinem Rücken, anstatt Euch wie versprochen gemeinsam um den Haushalt zu kümmern. Davon, dass es jetzt schneller geht, habe ich jedenfalls kaum etwas bemerkt. Dafür ist die Stromrechnung ein gutes Stück höher, und der Geräuschpegel sowieso. Außerdem musste ich noch ein Zimmer frei räumen, damit Ihr genug Platz habt. Langsam wird es eng.

Doch nicht genug damit, dass Du immer höhere Ansprüche stellst. Jetzt strebst Du auch noch danach, in die höhere Gesellschaft aufzusteigen. Mitglied im High Performance Club (HPC) willst Du werden. Du magst es ja als Selbstverwirklichung bezeichnen; für mich sieht es eher aus wie Torschlusspanik.

Wenn Du nur nicht so unzugänglich wärst. Hin und wieder erfahre ich zwar etwas über Dich, aber das sind meist alte Geschichten, die längst keine Bedeutung mehr haben. Wer Du heute wirklich bist, weiß niemand – am wenigsten ich.

Bevor mir der Kragen platzt, sage ich es lieber gleich, in aller Deutlichkeit: Ich habe die Nase voll. Ich will die Scheidung. Pack Deine Siebensachen und nimm auch Deine Schwester mit.

Den Einwand, ich käme ohne Dich nicht zurecht, habe ich erwartet. Weit gefehlt, mein Schatz. Eine junge Kollegin von mir würde liebend gern Deinen Platz einnehmen. Sie heißt Larrabee und ist nicht nur schlanker als Du, sondern kernig wie frisches Vollkornbrot. Obendrein talentiert und vielseitig – das liegt wohl in der Familie. Ihre älteren Geschwister zum Beispiel sind sehr erfolgreich.

Geheimnisse hat sie auch nicht – ich weiß alles über sie und ihre Verwandten. Nicht zuletzt, weil wir beide aus Santa Clara[3] stammen. Außerdem verstehen wir uns prächtig, wir sprechen nämlich dieselbe (Maschinen-) Sprache. Also mach keine Szene und verschwinde aus meinem Leben.

Michael Riepe

MICHAEL RIEPE



[1] AMD und Nvidia; [2] Scalable Link Interface; beide Techniken dienen zur Kopplung mehrerer Grafikkarten; [3] Firmensitz von Intel



Publishing für Profis

Äußerlich wenig verändert, soll Acrobat 9 den professionellen Anwender überzeugen. Beispielsweise hält sich die Publishing-Software an ISO-Standards und bietet bessere GIS-Funktionen. Spektakulär ist allein die Integration von Macromedias Flash-Technik.

Seite 62

Konserviert für die Ewigkeit

Die Archivierung von Geschäftsunterlagen wirft nicht nur technische Fragen auf, zahlreiche Gesetze und Richtlinien verkomplizieren die Sache. Ohne schlüssige Speicherstrategie kann sich ein IT-Leiter schnell zwischen Festplatten, optischen Medien und Bändern verlaufen. Orientierungshilfe ab

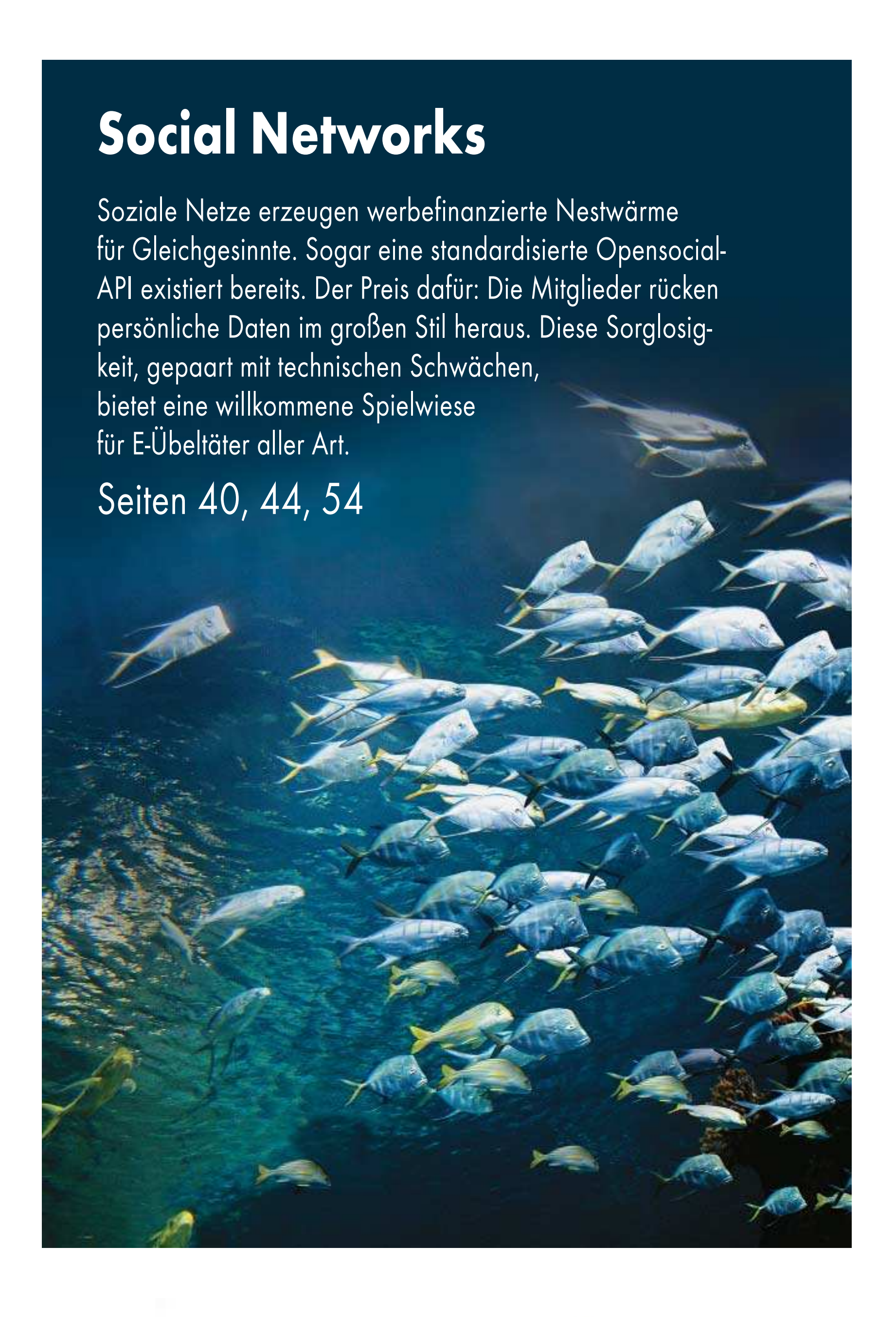
Seite 82



Anonym im Netz

Peer-to-Peer-Netze, die das Surfgebaren verschleiern, leiden allesamt unter systemimmanenten Schwächen. Nur ausreichend viele Teilnehmer erzeugen eine brauchbare Tarnkappe, und die Performance ist miserabel. Allein Open-Source-Varianten sind überhaupt zu empfehlen. Ein Überblick ab

Seite 88



Social Networks

Soziale Netze erzeugen werbefinanzierte Nestwärme für Gleichgesinnte. Sogar eine standardisierte Opensocial-API existiert bereits. Der Preis dafür: Die Mitglieder rücken persönliche Daten im großen Stil heraus. Diese Sorglosigkeit, gepaart mit technischen Schwächen, bietet eine willkommene Spielwiese für E-Übeltäter aller Art.

Seiten 40, 44, 54



Einladung zum Einbruch

Ein erfolgreicher Angriff brachte es ans Licht: Auch Kleinstcomputer sind nicht sicher – vor allem aus Kostengründen. Forscher knackten per Seitenkanalattacke das Keeloq-Verfahren, das Auto-, Garagen- und Haustüren per Funk öffnet.

Seite 121



Windows-Fan

(Editorial: Das Weiße im Auge; *iX* 8/08; S. 3)

Ich habe gerade Ihr Editorial in der neuen *iX* August 2008 gelesen. Warum schreiben Sie nicht ganz kurz: „Ich bin Windows-Fan und mit Apple möchte ich nichts zu tun haben.“ Man muss nicht immer ein Monopol unterstützen, sondern auch mal „anderen“ eine Chance geben.

HORST GROTH, RIETBERG

Der Autor des Editorials arbeitet mit einem Macintosh-Rechner. (d. Red.)



Pseudonym hat keine Meinung

(Recht: Wer darf oder muss Spuren im Internet löschen?; *iX* 8/08; S. 107)

Ihrer im vorletzten Absatz des oben genannten Artikels geäußerten **Meinung** möchte ich widersprechen. Eine Meinung definiert der Duden als „persönliche Ansicht“. Daher kann eine Aussage, die sich hinter einem (nicht auflösbaren) Pseudonym verbirgt, keine Meinung sein, da dieses Pseudonym keine Person darstellt. Dieses Pseudonym hat eher die Bedeutung einer Anonymität.

Damit relativiert sich entscheidend der Wert einer Aussage eines Pseudonyms. Anonymität ist keine Stärke sozialer Kompetenz, sie fördert Denunziantentum und verhindert Zivilcourage. Noch nie war es so einfach, ungestraft falsche oder widersprüchliche Aussagen zu veröffentlichen. Ist ein Pseudonym verschlissen, wird rasch eine neues erzeugt. Menschen, die eine Meinung haben und überzeugt sind, dass diese für andere wichtig ist, sollen diese gerne äußern können. Dann aber bitte so, dass sie auch persönlich für einen eventuell hervorgerufenen Widerspruch erreichbar sind.

Ist Ihnen eigentlich nie aufgefallen, welch gehaltloses Rauschen in Pseudonym-basierten Systemen vorherrscht? Vergleichen Sie einmal Blogsysteme mit den Leserbriefen Ihrer Tageszeitung und nicht zuletzt der *iX*. Was meinen Sie, was in letzteren los wäre, wenn jedes Pseudonym mit agieren könnte?

NIKOLAJ SCHUTZBACH, KONSTANZ

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

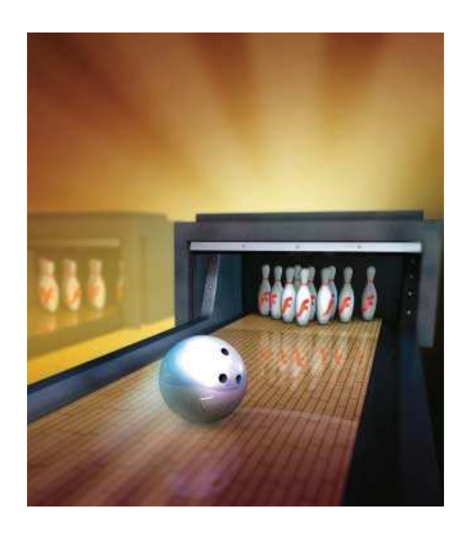
Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.



Thick Clients statt RIAs

(Rich Clients: Flex vs. Silverlight – Unterschiede und Gemeinsamkeiten; *iX* 8/08; S. 42)

Gerade habe ich oben genannten Artikel der *iX* mit großem Interesse durchgelesen, da die Firma, in der ich arbeite, sich auch mit Web Applications beschäftigt. Was ich sehr interessant fände, wäre eine Gegenüberstellung dieser RIA-Techniken und dem „reinem“ HTML+CSS+JS-Ansatz, wie man ihn letztens häufiger trifft, und den ich auf der WWDC von Apple als „Thick Clients“ bezeichnet gesehen habe. Wenn man sich die Homepage von Apple, das neue MobileMe oder auch nur einfach die Dia-Shows, die iWeb erzeugt, anschaut, stellt man fest, dass da keinerlei Plug-ins etc. genutzt werden (außer auf der Apple-Homepage für die Videos), sondern eigentlich alles mit HTML+CSS und Javascript realisiert wird und sich diese Web Applications in keinster Weise hinter den meisten Flash-Anwendungen verstecken müssen, weder was das Design, noch was die Nutzbarkeit angeht. (Die Suchfunktion des MobileMe-Adressbuchs ist wirklich sehr angenehm.) Gerade hinsichtlich des Faktes, dass JS-Interpreter immer schneller und mächtiger werden und eben keinerlei weiteres Plug-in benötigen, scheint mir ein Vergleich doch sehr interessant zu sein.

GREGOR KARZELEK, DARMSTADT

Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.

Wichtig: Die Anzahl der Zugriffe

(Speichersysteme: Erste 2,5-Zoll-SAS-Disk-Systeme im Test; *iX* 8/08; S. 80)

Ich habe eine Anmerkung zu dem Artikel. Beim Vergleich zwischen 2,5“- und 3,5“-Festplatten bzw. Storagesystemen vergleichen Sie lediglich die Speicherkapazität. Dass diese auf 2 U größer ist, will ich nicht bestreiten. Aber wie sieht es mit der Anzahl der möglichen IOPS aus? Wenn hier die 2,5“- und 3,5“-Festplatten ähnliche Werte je Festplatte aufweisen, so ist dies ein weiteres Argument für die 2,5“- Festplatten, da hier mehr IOPS im gleichen Volumen möglich sind.

Ich bestreite beinahe wöchentlich die Diskussion um die Frage, wie viele Festplatten müssen in einen Server, warum nimmt man nicht weniger und dafür größere Platten. Für die Performance von OLTP Datenbanken ist die Anzahl der Zugriffe wichtiger als die mögliche Übertragungsleistung, da jeder Zugriff nur wenig Daten liest oder schreibt.

Gibt es irgendwo einen Artikel, der sich dem Aspekt der maximalen Anzahl der möglichen Zugriffe widmet bzw. diesen Aspekt ebenfalls beleuchtet?

Ich möchte noch gerne die Möglichkeit wahrnehmen, ein Lob für die *iX* im Ganzen auszusprechen. Ich lese die *iX* sehr gerne, auch wenn ich längst nicht alle Artikel schaffe zu lesen (Zeitmangel). Vielen Dank und machen Sie so weiter!

Die Anregung wird gern aufgenommen. Ein entsprechender Artikel ist in Planung. (d. Red.)

Ergänzungen und Berichtigungen

(Websicherheit; Acht Web Application Firewalls; *iX* 8/08; S. 70)

Im Artikel wurden versehentlich Abbildung 2 und 3 vertauscht: Zur Bildunterschrift S. 71 gehört die Abbildung auf Seite 74 und umgekehrt.

(Vorschau; *iX* 8/08; S. 162)

Der im letzten Heft für diese Ausgabe angekündigte Testbericht des Apache-Moduls Modsecurity 2.5 kann aus redaktionellen Gründern leider erst im nächsten Heft erscheinen.

Black Hat und Defcon in Las Vegas

Duales System

Lukas Grunwald

Ob Vorratsdatenspeicherung oder RFID, E-Pass oder einheitliche Steuernummern: Digitalisierung und Verdatung der Gesellschaft nehmen Fahrt auf. Vor den damit einhergehenden Missbrauchsgefahren warnen Konferenzen wie die Black Hat und ihre kleine Schwester Defcon.

„Wann immer ich Blumen rieche, denke ich an Beerdigungen“ lautete der einleitende Satz von Ian Angell, Professor der London School of Economics, dessen Keynote-Rede zu den bisher eindrucksvollsten der Black Hat zählt. In einem sehr britischen und ziemlich düsteren Vortrag rechnete Angell mit der ausufernden Komplexität technischer Systeme ab.

Auf diese dennoch oder gerade deshalb unterhaltsame Einleitung folgten Beiträge, die sich mit den Details genau dieser Technik befassten. Die Black Hat erweitert ihr Spektrum immer stärker. Sieben parallele Vortragsreihen bereiteten den Zuhörern die Qual der Wahl, welchem Talk sie ihre Aufmerksamkeit schenken sollten.

Schlamperei bei Mautsystemen

Der Track „Over the Air“ etwa umfasste alle Themen von RFID über Software Defined Radio und Seitenkanalangriffe bis hin zum elektronischen Mautsystem. Mehrfach stand am Pranger, wie sehr die Produzenten von Mautsystemen in den USA geschlampt haben: Die aktiven RFID-Systeme von FastTrack und EZ-Pass sind aus der Ferne programmierbar, man kann die Kundennummern von Weitem auslesen, ändern und beliebig viel Unheil damit anrichten.

Virtuell unsicher

Daneben war die Sicherheit in der Virtualisierung ein großes Thema. Besonders der Xen-Hypervisor musste viele Schläge einstecken. In zwei Talks zeigten Rafal Wojtczuk und Johanna Rutkowska, wie er sich angreifen und manipulieren lässt. Schon traditionsgemäß führte Fyodor Vaskovich in seinem *nmap*-Beitrag auf, wie sich große Netze effizient scannen lassen, bis hin zum Worldscan-Projekt.

Zum ersten Mal auf der Black Hat fand sich dagegen die „Wall of Sheep“, ein virtueller Pranger für Nutzer des Black-Hat-Netzes, die ihre Passwörter nicht verschlüsselt hatten. Drei Reporter aus Frankreich ließen es sich angesichts dieser Verlockung nicht nehmen, ein ehernes Gesetz der Black Hat zu brechen und dort Passwörter von Kollegen zu publizieren. Während Scans und Angriffe im konferenzinternen Netz toleriert werden, gilt das davon getrennte Pressenetz jedoch als tabu für derlei Tätigkeiten – mit der Folge eines lebenslangen Hausverbots auf der Black Hat und der Defcon für das spionierende Trio.

Jeroen van Beek machte dort weiter, wo die Black Hat 2006 in Sachen E-Pass endete: Er zeigte, dass sich auch die neu eingeführten Sicherheitsmaßnahmen wie „Active Authentification“ aushebeln lassen und dass E-Pässe mit selbstsignierten Schlüsseln von Lesesystemen in den Bürgerämtern in den Niederlanden sowie dem europäischen Golden Reader Tool akzeptiert werden. Mit einem Bin-Laden-Pass, den das niederländische Inspection System anerkannte, löste er einigen Trubel aus – wie auch mit einem Elvis-Pass, passend zum Veranstaltungsort Las Vegas.

Per Funk einbrechen und stehlen

Karsten Nohl verdeutlichte einmal mehr, dass man durch Geheimhaltung von Algorithmen („Security by Obscurity“) keine dauerhafte Krypto-Sicherheit erreichen kann. Per Reverse Engineering zeigte er, dass der RFID-Chip Mifare nur zwei lineare Schieberegister benutzt, sodass sich Mifare-Karten und damit etliche drahtlose Zugangssysteme, etwa von ferngesteuerten Garagentoren, Autos und Bezahlsystemen, leicht entschlüsseln lassen.



Inhaltliche Qualität und damit der praktische Nutzen dagegen waren, mit wenigen Ausnahmen, sehr hoch. Bei allem Erfolg hatte die Black Hat aber auch Schattenseiten: Mit fast 5000 zahlenden Besuchern war die Konferenz total überfüllt. Zwischen den Vorträgen dauerte es bis zu 20 Minuten, den Raum zu wechseln, und das Hotel war mit dem Catering überfordert.

Embedded-Computer als Defcon-Ticket

Kurz nach der Black Hat startete traditionsgemäß die wesentlich erschwinglichere Hacker-Konferenz Defcon. Für 100 US-Dollar Eintrittspreis bekam jeder Teilnehmer als Ausweis einen Embedded-Computer von Freescale – diesmal mit stärkerer Batterie, die das komplette Wochenende durchhielt. Diese Eintrittskarten erzielen bei Ebay deutlich höhere Preise. Sie enthalten einen SD-Speicherkartenleser und erlauben neben dem Datenaustausch mit anderen Defcon-Teilnehmern – drahtlos per Infrarot – das Ausschalten aller Fernsehgeräte in Sichtweite. Zum Erweitern und Umprogrammieren hat der Entwickler Kingpin (demnächst mit eigener TV-Show) ein Codewarrior Development Studio for Microcontrollers beigelegt sowie alle Datenblätter und den kompletten Software-Quellcode.

Auch die Defcon hatte Neuigkeiten zum Thema Port-Scanning im Programm – in Form von Portbunny aus Deutschland. Das kernelbasierte Netz-Analysewerkzeug arbeitet gefilterte Hosts wesentlich schneller ab als eines, das wie *nmap* im Userspace läuft.

Neben vielen weiteren Informationen zu Privacy, WLANs, Social- und Byte-by-Byte-Hacking bot die Defcon leider auch einiges Halbwissen angetrunkener Twens am Rednerpult. Beeinträchtigungen erfuhr die Black-Hat-Schwesterveranstaltung wieder einmal durch den Arm des Gesetzes: Ein Vortrag fiel einer einstweiligen Verfügung zum Opfer. Die Bostoner Verkehrsbetriebe (MTBA) stoppten die Ausführungen von MIT-Studenten über die schon lange geknackte Charlie Card, die auf dem Mifare-Chip von NXP basiert. Angeblich gefährdeten diese Informationen die öffentliche Ordnung und Sicherheit. Stattdessen gab es einen passenden Vortrag der Electronic Frontier Foundation über die Redefreiheit.

Angesichts der Tatsache, dass die Defcon in mancher Hinsicht einen zweiten Aufguss der Black Hat realisiert, waren dort richtige Neuerungen im IT-Sicherheitsbereich nicht zu erwarten. Vielmehr stand die Unterhaltung der Teilnehmer im Mittelpunkt. So konnte, wer zu viel von IT und Computern hatte, im Rahmen des Wi-Fi Shootout in der Wüste Nevadas neben großen Richtantennen auch großkalibrige Automatikwaffen testen. (un)

PostgreSQL-Client für das iPhone

Mobilecan (s. *iX*-Link) ist eine abgespeckte Variante des freien PostgreSQL-Client Oilcan, der auf dem iPhone läuft. Mit ihm lassen sich einfache Abfragen erstellen und ausführen. Außerdem kann man, geeignete Rechte vorausgesetzt, Prozesse innerhalb der Datenbank abbrechen. Bislang kann man die Parameter einer Verbindung nicht mehr ändern, sondern muss sie insgesamt löschen und neu anlegen. Mobilecan liest immer 20 Datensätze auf einmal vom Server; Felder mit 30 oder 40 KByte können deshalb seinen Speicher erschöpfen.



SQL Server 2008 ist fertig

Microsofts SQL Server 2008 ist mit einem halben Jahr Verspätung erschienen. Bis auf die Express-Version sind alle Varianten erhältlich: Developer, Standard, Web, Workgroup, Enterprise und Compact. Der kostenlose, aber im Funktionsumfang eingeschränkte SQL Server 2008 Express soll Ende August herauskommen.

Als Neuerungen hebt Microsoft Änderungen für Data Warehouses und Reporting-Funktionen hervor. Per „Change Data Capture“ lassen sich alle Datenbankänderungen in Tabellen speichern, die für SQL-Befehle zugänglich sind. Dadurch können Data Warehouses schneller befüllt werden, da man nur noch die Änderungen gegenüber dem letzten Export übertragen muss. Wer die Reporting Services (SSRC) benutzen will, muss dafür jetzt nicht mehr Microsofts Webserver IIS einsetzen. *MERGE* ist ein neu eingeführter SQL-Befehl, der standardkonform einen Datensatz aktualisiert oder ihn anlegt, wenn er noch nicht existiert.

Programmierern verschaffen automatisch erzeugte System-Views einen Überblick über die Abhängigkeiten zwischen Objekten wie Stored Procedures, Tabellen, Views, Funktionen, Triggern und so weiter. Das automatische Vervollständigen verschiedener Sprachelemente (unter anderem Schlüsselwörter) funktioniert erstmals mit T-SQL. Für Datum und Zeit stehen zwei getrennte Datentypen zur Verfügung. *geometry* und *geography* speichern geografische Daten und orientieren sich dabei an den Vorgaben des Open Geospatial Consortium.

Sicherheitslücken in Ingres und SAPs MaxDB

Laut iDefense enthält die SAP-Datenbank MaxDB eine Lücke, mit der ein Angreifer weiterreichende Rechte erlangen kann. Beim Start per *dbmcli* prüfe die *dmbsrv*-Anwendung den *PATH* nicht hinreichend. Deshalb könnten Angreifer mit einer manipulierten *PATH*-Variablen beliebigen Code mit den Rechten des Benutzers *sdb* ausführen. Der Fehler existiert in MaxDB 7.6.03.15 unter Linux; SAP hat eine korrigierte Version veröffentlicht.

Ebenfalls auf eine mangelhafte Prüfung der *PATH*-Variablen geht ein Fehler in Ingres zurück. Außerdem gibt es dort einen Buffer Overflow. Er ermöglicht das Einschleusen und Ausführen von Code mit den Rechten des Datenbank-Eigentümers (*ingres*). Die Bugs stecken in Ingres 2006 Release 2 (9.1.0), Release 1 (9.0.4) und in Ingres 2.6. Korrigierte Versionen gibt es beim Ingres Service Desk.



Codefork bei MySQL: Drizzle speckt ab

Brian Aker hat eine Abspaltung vom MySQL-Projekt unter dem Namen Drizzle initiiert. Ziel ist es, eine schnelle Datenbank für Webanwendungen zu erstellen, die ohne Transaktionen, Stored Procedures und andere unternehmenskritische Features auskommt. Alle Codeteile sollen offen liegen und in einem transparenten Entwicklungsprozess entstehen.

Wertvolle Informationstechnik

Die Frage, welche IT-Ausgaben sinnvoll sind, will das IT Governance Institute (ITGI) mit dem Val IT Series Enterprise Value beantworten, einem Steuerungsinstrument für IT-Investitionen. Das Framework, das auf www.itgi.org zum kostenlosen Download verfügbar ist, umfasst allgemein akzeptierte Leitlinien und bewährte Praktiken, die die Rendite im IT-Bereich maximieren.

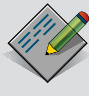
Die Version 2.0 von Val IT enthält unter anderem Wertschöpfungs-Steuerungsprozesse, die nun auch IT-Dienstleistungen, Anlagen et cetera umfassen sowie Managementrichtlinien für jeden Val-IT-Prozess (einschließlich Inputs und Outputs zu/von jedem Prozess). Hinzu kommen detaillierte Reifegrad-Modelle für die drei Val-IT-Domänen Wertschöpfungs-Steuerung, Portfolio- und Investitionsmanagement. Die Terminologie fußt auf COBIT (Control Objectives for Information and Related Technology), dem Framework zur IT-Governance. COBIT stammt wie Val IT aus der Feder des ITGI. Während Val IT zu Investitionsentscheidungen und der Realisierung von Gewinnen beitragen soll, legt COBIT die Steuerungsvorgaben fest. Das ITGI ist ein unabhängiges Forschungsinstitut und gehört zum internationalen Verband der IT-Prüfer ISACA (www.isaca.org).

Monitoring aus der Anwenderperspektive

Attachmates Tochter NetIQ bringt ein neues Appmanager Response Time Module for Windows auf den Markt. Das Werkzeug erlaubt Beurteilungen der Qualität von IT-Services aus der Sicht von Endanwendern, die Windows einsetzen. Es erfasst nicht nur Applikationen wie Microsofts Exchange (via Outlook), Sharepoint, Siebel und SAP, sondern auch selbstentwickelte Anwendungen oder Desktop-Applikationen. Appmanager führt synthetische Transaktionen aus, die das Endbenutzerverhalten auf dem Windows-Desktop mit Mausklicks oder Dateneingaben emulieren.

Änderungen der zu steuernden Oberflächen erkennt das System mittels Zeichenerkennung und Bitmap-Vergleichsverfahren automatisch. Administratoren können den Ablauf einer Transaktion über ein GUI ändern. Die Listenpreise beginnen bei 2535 Euro pro zu überwachendem Endpunkt.

KURZ NOTIERT



Ergänzt: Nimsoft erweitert sein gleichnamiges Kernprodukt um eine passive Monitoring-Lösung auf Basis der im April erworbenen Indicative-Software. Eine Appliance namens Real User Monitoring (RUM) analysiert den Datenstrom innerhalb einer Webanwendung und ermittelt unter anderem Zahlen zu Transaktionszeiten und Übertragungskapazitäten.

Ressourcen im Blick: Hyperic hat die gleichnamige Managementsoftware auf die Verwaltung von Xen-Server ausgedehnt. Mittels Plug-in lassen sich virtuelle Serverinfrastrukturen auf dessen Basis mit Hyperic HQ verwalten.

Erweitert: Beta Systems hat ihre Produktsuite Beta UX ausgebaut: Neben UC4, Dollar Universe und J2U verfügt die Komponente History Management nun über Standardkomponenten zur Verarbeitung von Log-Typen der Scheduling-Systeme IBM TWS for Distributed, BMC Control/M und Sun MBM.

Lückenschluss: ASG Software Solutions baut sein Angebot an Business-Service-Management (BSM) aus und führt Performance-Indikatoren von Mainframe- und von dezentralen IT-Systemen zusammen. TMON von ASG unterstützt, verbunden mit Microsofts System Center Operations Manager, z/OS-Rechner sowie dezentrale, virtualisierte, J2EE- und .Net-Systeme.

Schnelleres Rendering mit Cinema 4D R11

Die deutsche Maxon GmbH hat die Siggraph, die weltgrößte Konferenz zu Computergrafik und Animation, zum Anlass genommen, eine neue Version ihrer Animationssoftware vorzustellen (siehe *iX*-Links). Teil von Cinema 4D Release 11 sind ein nichtlineares Animationssystem und eine neue Render Engine für globale Beleuchtung. Laut Hersteller ist das Rendering mit der neuen Version deutlich schneller. Das zum RenderMan-Standard kompatible CineMan ermöglicht die Anbindung entsprechender Renderer.

Außerdem in der neuen Version enthalten ist das von Maxon für Sony Pictures entwickelte Matte Painting System für Füll- und Hintergrundbilder im digitalen Compositing. Als Austauschformat für 3D-Daten nutzt Cinema 4D das von der Khronos Group gerade in der Version 1.5.0 verabschiedete Collada. Maxon hat angekündigt, die neue Version im September auszuliefern.



Autodesk stellt Maya 2009 vor

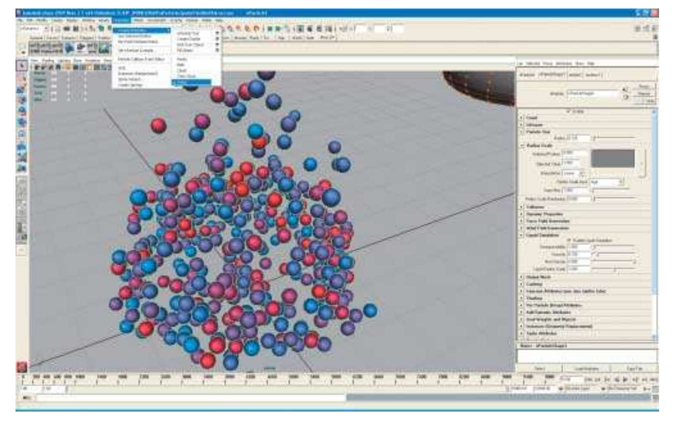
Zur Feier des 10-jährigen Jubiläums ihrer Animationssoftware hat Autodesk auf der Siggraph in Los Angeles die Version Maya 2009 präsentiert (www.autodesk.com/maya). Zu den Neuerungen zählt das Modul nParticles (siehe Abbildung), das Teil des Nucleus Unified Simulation Framework ist. Es vereinfacht die Simulation komplexer physikalischer Effekte, beispielsweise Rauch oder Gischt, und erlaubt die Interaktion zwischen einzelnen Partikeln. Speziell der realistischen Darstellung von Haut und Muskeln sowie deren durch Bewegung bedingte Veränderungen dient Maya Muscle.

Maya Assets soll den Anwendern zudem helfen, komplexe Daten effektiv zu verwalten. Anwender können damit einen Satz von Knoten in einem Container zusammenfassen und sie wie einen einzigen Knoten behandeln. Das erlaubt unter anderem benutzerspezifische Views sowie anwendungsspezifische Bibliotheken. Die neue Render-Proxy-Funktion in Mentalray, der in der neuen Version 3.7 in Maya 2009 integriert ist, erlaubt es, einzelne Elemente einer Szene zunächst in einer einfachen Auflösung darzustellen und die kompletten Daten bei Bedarf nachzuladen.

Die neue Version der Animationssoftware soll im Oktober im Handel sein (zunächst nur in der englischen Fassung). Als Preise nennt Autodesk 2225 € für Maya Complete 2009 und 5575 € für die Unlimited-Version. Upgrades kosten 1000 beziehungsweise 2000 €.

Ebenfalls im Oktober im Handel soll Motionbuilder 2009 sein. Die Software dient der Animation dreidimensionaler Figuren für Spiele- und Filmprojekte. Ein intuitives Simulationswerkzeug in Echtzeit sowie erweiterte Scripting-Fähigkeiten ergänzen die neue Version. MotionBuilder 2009 kostet 4475 €, ein Upgrade ist für 1125 € zu haben.





Collada 1.5.0: Lingua Franca für 3D-Designer

Die Khronos Group hat die Version 1.5.0 von Collada verabschiedet (www.khronos.org/collada/). Das XML Schema (XSD) ist ein Austauschformat für 3D-Inhalte, das mittlerweile viele Animations- und Grafikprodukte unterstützen, darunter Softimage XSI, Maya, 3DS Max, Googles Sketchup, Nvidias FX Composer 2 und Photoshop CS3.

Ergänzt wurde die Spezifikation um B-reps (Boundary Representations) und Kinematik-Funktionen, die unter anderem in der Automotive-Industrie von Bedeutung sind. Neu ist außerdem ein Profil für Effekte in OpenGL ES 2.0 (Open Graphics Library for Embedded Systems), darüber hinaus hat das Konsortium die Unterstützung für externe Shader-Systeme verbessert. Da Collada 1.5.0 Georeferenzierung räumlicher Daten unterstützt, können GIS-Anwendungen mithilfe dieses Formats reale und virtuelle 3D-Daten gemischt verwenden. Ein neues, unter Mitarbeit von Google entwickeltes Dateiformat mit der Endung .zae (Zipped Asset Exchange) ist dafür gedacht, komprimierte Collada-Modelle über Googles 3D Warehouse zugänglich zu machen.

Gleichzeitig mit der neuen Release der Spezifikation hat die Khronos Group ein Update für die Vorgängerversion verabschiedet. Collada 1.4.2 enthält Fehlerkorrekturen und kleinere Zusätze.



Spiele entwickeln mit Tools von Nvidia

Neue Versionen zweier Werkzeuge sowie ein zusätzliches Plug-in sollen Spieleentwicklern das Leben leichter machen. Für das Debugging und die Performance-Analyse von DirectX-9- und DirectX-10-Anwendungen hat Nvidia die Version 6 von PerfHUD vorgestellt. Die neue Release unterstützt GPUs mit Nvidias SLI-Technik und bietet diverse Programmierschnittstellen.

Eine Überarbeitung hat die Benutzeroberfläche der IDE FX Composer erfahren. Die Version 2.5 enthält außerdem visuelle Modelle, Styles sowie Partikelsysteme und unterstützt DirectX 10. Für das Debugging und die Optimierung von Shadern, die mit HLSL, GcFX oder Collada FS Cg in DirectX oder OpenGL programmiert wurden, stellt Nvidia den Shader Debugger, ein Plug-in für den FX Composer 2.5, zur Verfügung (developer.nvidia.com).



Khronos Group verabschiedet OpenGL 3.0

Rechtzeitig zur Siggraph hat die Khronos Group die neue Spezifikation des plattformübergreifenden 3D-Standards OpenGL verabschiedet (www.khronos.org/opengl/). Viele neue Funktionen sollen vor allem der Spieleentwicklung zugutekommen. Unter anderem erlauben Arrays mit 32-Bit-Gleitkomma-Elementen die präzisere Darstellung von Texturen. Von Occlusion Queries (Abfragen auf Verdeckung) abhängiges Rendering soll die Performance verbessern. Das Rendering in sRGB-Framebuffers erlaubt die farbechte Wiedergabe von OpenGL-Anwendungen, ohne dass eine Gamma-Korrektur des Monitors nötig ist.

Die neue Version der OpenGL Shading Language, GLSL 1.3.0, verbessert unter anderem die Kompatibilität zu OpenGL ES, dem OpenGL-Standard für Embedded-Systeme. Neben Extensions für die neue Release hat die Khronos Group Erweiterungen für OpenGL 2.1 verabschiedet, die es erlauben, die neuen Funktionen auch mit älterer Hardware zu nutzen.

AMD, Intel und Nvidia, die an der Spezifikation mitarbeiteten, haben bereits bekannt gegeben, dass sie OpenGL 3.0 in ihren Produkten unterstützen wollen.



Ruhe und Unruhe um das freie Handy-Betriebssystem Android

Fans des von Google mit viel Brimborium angekündigten freien Handy-Betriebssystems Android zeigen sich vom Entwicklungstempo enttäuscht. In einer Online-Petition beklagten sie sich darüber, dass es seit Anfang März keine neue Version des Entwicklungs-Kit gegeben hat (s. *iX*-Link). Fehler etwa im Mediaplayer würden nicht korrigiert, angekündigte Features wie Geokodierung nicht implementiert. Android ist eine Linux-Variante. Anwendungen dafür sollen in Java geschrieben werden.

Wenige Wochen später dementierte der chinesische Gerätehersteller HTC Verzögerungen bei der Produktion des ersten Android-Handys: Es werde wie angekündigt im vierten Quartal 2008 erscheinen. Ein amerikanisches Blog hatte einen Analysten zitiert, demzufolge HTC Googles technische Anforderungen nicht erfüllen könne. Ursprünglich sollte das erste Android-Handy im zweiten Quartal dieses Jahres fertig sein.

Der erwähnte Analyst bezweifelte außerdem, dass Android genügend Entwickler mobilisieren könne. Konkurrierende Plattformen hätten schon funktionierende SDKs.



IPSec für Symbian

Die Nürnberger Firma NCP engineering hat einen IPSec-Client mit integrierter Firewall für Symbian-Handys der S60-Reihe vorgestellt. Er unterstützt VPN-Verbindungen über WLAN und GSM/UMTS mit vorher festgelegten Schlüsseln (pre-shared key, PSK). In einer der nächsten Versionen soll es außerdem möglich sein, Zertifikate zu nutzen.

Zur Einstellung des Clients ist ein Windows-PC unabdingbar: Die Konfigurationssoftware läuft nur dort und benötigt für die Übertragung der Parameter zum Mobiltelefon Nokias Synchronisationssoftware PC-Suite. In größeren Installationen lässt sich alternativ eine Verwaltungssoftware von NCP einsetzen.

Eine 30 Tage lauffähige Testversion des Clients samt der Anwendung zum Einrichten ist online verfügbar (s. *iX*-Link).



Mobilfunk billiger

Wie angekündigt, sinken die Tarife für Handytelefonate in der EU in diesem Sommer erneut: Ab 30. August kostet ein abgehendes Gespräch noch 0,46 € pro Minute, für ankommende werden 0,22 fällig (jeweils zuzüglich MwSt.). EU-Kommissarin Viviane Reding setzt zudem die Mobilfunkanbieter weiter unter Druck, die Roaming-Gebühren für SMS und anderen Datenverkehr zu senken. Eine SMS kostet innerhalb der EU zurzeit im Durchschnitt 28 Cent, Reding hält rund 12 Cent für angemessen. Sollten die Unternehmen die Preise nicht von sich aus senken, will Reding sie per Verordnung reduzieren.



iX-Veranstaltungen

www.ix-konferenz.de

Wie an dieser Stelle bereits erwähnt, findet heuer zum zweiten Mal die Konferenz zum Thema Subversion statt, die **SubConf 2008** (14. bis 16. Oktober, München). Die Veranstalter, Hood, HLMC und *iX*, freuen sich, wieder einige der Core Committer von Subversion in München begrüßen zu dürfen. Auch in diesem Jahr wird Karl Fogel, President Subversion Corporation und Subversion Committer, die Keynote halten.



Keynote-Speaker auf der SubConf 2008: Karl Fogel

Zudem erhält die SubConf eine Schwesterkonferenz, die parallel stattfindet: die **CMConf 2008** zum Themenkomplex „Configuration, Change und Version Management“. Teilnehmer der SubConf 2008 können kostenlos die Vorträge der CMConf 2008 besuchen und vice versa. Wer sich vor dem 1. September anmeldet, spart 200 Euro – netto.

Auch das Programm für den **Software-QS-Tag 2008** ist weitgehend in trockenen Tüchern. Die von der Imbus AG seit 16 Jahren veranstaltete und erstmalig von *iX* unterstützte Konferenz zum Thema „Softwarequalitätssicherung und -testen“ steht in diesem Jahr unter dem Motto „Model based Testing“. Der „eigentliche“ QS-Tag findet am 6. November in Nürnberg statt, am Tag davor und danach gibt es Workshops zum Thema.

Eine von uns mitverantwortete Konferenz, die TeamConf zu Microsofts Visual Studio Team System, hat einen Ableger bekommen, an dem wir nicht direkt beteiligt sind: die TeamConf Schweiz (1. bis 3. Dez. 2008, www.teamconf.ch).

WLANs müssen durch Verschlüsselung geschützt sein

Die Frage nach der Verantwortlichkeit von Betreibern „offener“ Funknetze beschäftigt derzeit etliche Gerichte. Meist handelt es sich um Fälle, bei denen einem WLAN-Besitzer (urheber-)rechtswidrige Downloads angelastet werden, die dieser aber gar nicht selbst, sondern ein Dritter unter Nutzung der IP-Adresse des Betreibers vorgenommen hat. Streitig ist dann die Frage, ob der Betreiber trotzdem haftet, weil er seinen Hotspot nicht ausreichend gegen die Nutzung durch Dritte abgesichert hat. Das Landgericht Düsseldorf hat nun entschieden, dass ein Anschlussinhaber zumindest Maßnahmen zur Verschlüsselung des Funknetzes ergreifen muss (Az. 12 O 195/08).

Andernfalls „verschafft er nämlich objektiv Dritten die Möglichkeit, sich hinter seiner Person zu verstecken und im Schutze der von ihm geschaffenen Anonymität ohne Angst vor Entdeckung ungestraft Urheberrechtsverletzungen begehen zu können“, so die Richter. Der Anschlussinhaber ist damit Störer im rechtlichen Sinne, was seine Inanspruchnahme auch ohne eigenes Verschulden ermöglicht. Nach einer Entscheidung des Bundesgerichtshofs gilt als Störer, „wer in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechtsguts beigetragen und zumutbare Sicherungsmaßnahmen unterlassen hat.“ Welche Maßnahmen konkret zu ergreifen sind, hat das Gericht nicht entschieden, da im vorliegenden Fall klar war, dass es überhaupt keine Schutzvorkehrungen gab. *Tobias Haar*

EU-Forschungsgelder für optische WDM-Netze

Das von der EU mit 3 Millionen Euro unterstützte Gigawam-Projekt soll die Kosten für die optische Breitbandverkabelung drastisch senken. Dazu entwickelt ein Konsortium aus vier Firmen neue, höher integrierte WDM-PON-Komponenten (Wavelength Division Multiplexing/Passive Optical Networking). Das Projekt läuft bis März 2011. Ziel ist es, die für das Streaming von Multimediadaten nötige Übertragungskapazität von mindestens 1 Gbps möglichst günstig bereitzustellen. Bislang sind WDM-Komponenten zwei- bis dreimal so teuer wie das Time Multiplexing Gigabit Passive Optical Network (GPON). Insgesamt wollen die beteiligten Firmen Ignis Photonyx aus Dänemark, Ericsson aus Schweden, Vertilas und Ficontec aus Deutschland 9 Millionen Euro in das Projekt investieren. Sie hoffen auf Umsätze mit der Technik in Höhe von 230 Millionen Euro im Jahr 2013.

iPhone-Werbung der Telekom teilweise rechtswidrig

Das Landgericht Hamburg hat der Deutschen Telekom bestimmte Werbeaussagen im Zusammenhang mit der Bewerbung ihres iPhone-Tarifs „Complete“ untersagt (Az. 315 O 360/08). Sie darf diesen Tarif nicht mehr als „freien Internetzugang mit unbegrenzter Datenflatrate“ bewerben.

Die Klägerin – ein Voice-over-IP-Anbieter – hatte argumentiert, dass der Internetzugang keineswegs frei sei. VoIP-Verbindungen sind nämlich unzulässig. Das Gleiche gilt für Instant-Messenger-Protokolle und verschlüsselte Tunnel (VPN). Auch die Aussage, es handle sich um eine unbegrenzte Flatrate, trifft nach Aussage der Klägerin nicht zu. Denn die Übertragungskapazität des Zugangs wird ab einem Volumen von 5 GByte (Complete XL) oder schon 300 MByte (Complete M) auf ISDN-Durchsatz reduziert. Daher sind „zahlreiche Dienste, beispielsweise Internetradios oder Videofilmstreams, gar nicht oder nur erheblich eingeschränkt nutzbar“, so die Klägerin. Dieser Auffassung haben sich die Richter angeschlossen. Die Deutsche Telekom hat daraufhin ihre Werbung entsprechend geändert. *Tobias Haar*

Zweispurig zum neuen Internet-Protokoll IPv6

Auf dem Treffen der Internet Engineering Task Force (IETF) Ende Juli in Dublin kamen erneut Übergangsszenarien zu IPv6 zur Sprache. Voraussichtlich sind im Jahr 2011 keine IPv4-Adressen mehr verfügbar. Neue IP-Adressen stehen dann nur noch für das neue Protokoll zur Verfügung. IETF-Fachleute erwarten ein vorübergehendes Nebeneinander von IPv4 und IPv6. Tunnel gibt es bereits seit Jahren, so Fred Baker von Cisco, Chef der IETF-Arbeitsgruppe IPv6 Operations. Sie übersetzen allerdings die Protokolle nicht ineinander, sodass der IETF kaum Alternativen zur eigentlich ungeliebten Network Address Translation (NAT) bleiben dürften, die bereits unter IPv4 als Notbehelf gilt.

Ein Vorschlag von Comcast-Ingenieur Alain Durand namens „Dual-Stack lite“ soll IP4-Daten vom und zum Breitbandkunden durchs IPv6-Netz des Carriers tunneln. Ein IPv4-IPv4-NAT im Carriernetz setzt die privaten IP-Adressen in global routbare um. IPv4-Ressourcen im Internet bleiben für die Kunden auch dann erreichbar, wenn es keine neuen IPv4-Adressen mehr gibt. Durand sieht den Vorteil, dass auf diese Weise nicht mehrere NAT-Schichten erforderlich seien. NAT aufseiten der Carrier schlagen auch Entwickler von NTT vor, wenn auch ausdrücklich als Übergangslösung.

Nach Meinung von Baker kann providerseitige NAT die Einführung von IPv6 höchstens um ein bis zwei Jahre hinauszögern. Auch Gert Döring ist dieser Meinung. Sein Arbeitgeber Spacenet stattet Kunden auf Wunsch bereits mit IPv6-Adressen aus.

Alte Freunde großer Systeme

Nachdem das rechtliche Gerangel kein befriedigendes Ergebnis brachte, kauft IBM die Plattform Solutions Inc. (PSI) auf. Das Unternehmen bietet unter anderem Emulatoren für das Mainframe-Betriebssystem z/OS auf Standardprozessoren (Itanium 2) an. Die Mitarbeiter und Produkte von PSI werden folgerichtig der System-z-Sparte von IBM zugeschlagen. Ein pittoreskes Detail der Übernahme ist die Gründungsgeschichte von PSI. Diese ist eng verknüpft mit Gene Amdahl. Der promovierte Wissenschaftler war einst bei IBM angestellt und gilt als Vater des Systems-360-Mainframe. 1970 gründete Amdahl dann ein eigenes Unternehmen, das seinen Namen trug, zum ärgsten Konkurrenten von IBM im Geschäft mit kompatiblen Großrechnern wurde und heute im Besitz von Fujitsu ist. Aus dem Kreis der Amdahl-Mitarbeiter machte sich 1999 ein Entwicklerteam selbstständig, um PSI zu gründen. Gene Amdahl begleitete die Neugründung als Berater.

Studien zur IT in Krankenhäusern

IT in Krankenhäusern kann Ärzte bei der Heilung von Patienten unterstützen und gleichzeitig durch eine Optimierung interner Geschäftsprozesse Kosten sparen. Eigentlich nichts Neues. Diese Erkenntnis ist aber noch längst nicht zu allen IT-Entscheidern in Krankenhäusern durchgedrungen, wie Marktforscher von IDC Central Europe GmbH ermittelt haben. 75 Prozent schöpfen das Potenzial der IT noch längst nicht aus, bei acht Prozent liegt es weitgehend brach. 17 Prozent konnten in strukturiert geführten Telefoninterviews von sich sagen, dass sie die Chancen nutzen.

Für die Studie „Die Rolle der IT im Gesundheitswesen – Status Quo und Trends in deutschen Krankenhäusern, 2008“ befragte IDC 52 IT-Verantwortliche aus privaten und öffentlichen Krankenhäusern unterschiedlicher Größe. Zielgruppe sind IT-Anbieter, die in dieser zwar attraktiven, aber von Gesundheitsreform und Geldknappheit geplagten Branche tätig sind oder dies planen. Damit sie ihre Angebote möglichst genau auf ihre potenziellen Kunden ausrichten können, analysieren die Marktforscher zum Beispiel den Stellenwert von IT in den Kliniken. Hier gibt es Defizite sowohl in der IT-Abteilung, bei Anwendern und in der Geschäftsführung. Die Studie kostet netto 3900 Euro und ist über www.idc.com zu beziehen.

In die gleiche Richtung weisen Ergebnisse einer Studie von SAP und Accenture. Die Beteiligten sehen ein Sparpotenzial von 400 Mio. Euro jährlich, wenn Krankenhäuser und niedergelassene Ärzte einheitliche IT-Plattformen nutzen würden. *Barbara Lange*

iX-Umfrage: Thin Clients werden mehrheitsfähig

Überraschend häufig werden nach den Ergebnissen unserer Online-Umfrage, die parallel zu Heft 8/08 auf www.ix.de lief, Thin Clients eingesetzt. Über ein Drittel der Antwortenden hat sie bereits im Einsatz, 12 Prozent planen dies. Aber: Immerhin noch 16 % wussten mit den Begriff nichts anzufangen.

Details sind der nebenstehenden Grafik zu entnehmen. Die nächste Umfrage, die ab dem 20. August online ist, wird sich mit dem Thema Mainframes beschäftigen.

Was halten Sie von Thin Clients als Arbeitsplatzsytem?

Antwort	Anteil
Thin Clients sind bei uns in der Firma breit im Einsatz	20 %
Wir haben einige wenige Arbeitsplätze mit Thin Clients ausgerüstet	16 %
Der Einsatz von Thin Clients ist geplant	12 %
Thin Clients kommen für uns nicht infrage	36 %
Was sind überhaupt Thin Clients?	16 %

Gesamtstimmen: 470 (gerundet)

US-Zoll darf Laptops durchsuchen

In einer offiziellen Erklärung hat das US-Heimatschutzministerium bestätigt, dass Bundesbeamte bei Zollkontrollen Daten auf Notebooks und anderen elektronischen Geräten wie etwa MP3-Playern oder Mobiltelefonen und Datenträgern bis hin zu Audiokassetten oder Notizblöcken durchsuchen dürfen. Auch die Anfertigung von Kopien der gespeicherten Daten ist zulässig. Brisant dabei: Solche Kopien darf der Zoll an Unternehmen weitergeben. Namentlich nannte die Behörde als Gründe, die eine solche Weitergabe rechtfertigen, das Erfordernis, eine Verschlüsselung knacken zu müssen, fremdsprachliche Inhalte übersetzen lassen zu müssen, aber auch „andere Gründe“.

Von den Zollbehörden eingezogene Geräte müssen aber innerhalb einer „angemessenen Frist“ wieder zurückgegeben werden, was in Einzelfällen auch schon mal Monate dauern kann. *Tobias Haar*

E-Government-Gesetz

Als erstes Bundesland hat Schleswig-Holstein einen Entwurf für ein Gesetz zur elektronischen Verwaltung des Landes vorgestellt, das sogenannte E-Government-Gesetz (EgovG): Demnach sollen Städte und Gemeinden in Zukunft einheitliche IT-Infrastrukturen nutzen. Noch arbeiten Land, Kreise, Gemeinden und andere Behörden mit unterschiedlichen elektronischen Verfahren. Nach Angaben des Schleswig-Holsteinischen Finanzministeriums wollen die Nordlichter nun gemeinsame Infrastrukturen, Basisdienste, Datenformate und Schnittstellen schaffen, um sowohl untereinander als auch mit Bürgern und Unternehmen einheitlich kommunizieren zu können. Das neue Gesetz soll sicherstellen, dass die Verwaltungen ihre elektronischen Verfahren so aufeinander abstimmen, dass alle betroffenen Stellen die Daten ohne Komplikationen verarbeiten können. So sollen Doppelerfassungen der Vergangenheit angehören. *Barbara Lange*



Dell startet HPC-Pilotprogramm

Vorkonfigurierte Supercomputer zum erschwinglichen Preis will Dell (www.dell.com/hpcc) gemeinsam mit mehreren europäischen Partnern entwickeln. Dazu hat das Unternehmen ein Pilotprogramm angekündigt, das noch im Herbst starten soll. Als Basis dienen Dells Bladesysteme „PowerEdge M“. Der Cluster kann aus 4 bis 32 Knoten bestehen, die unter Red Hats Enterprise Linux laufen. Noch in diesem Jahr soll es das HPC-System auch mit Windows geben.

An dem Programm beteiligen sich die TUs Dresden und Berlin, die Katholische Universität Leuven (Belgien), die britische Bankenkette No 1 Currency, aus Frankreich die Entwickler für Simulationssoftware Insilico, das europäische Institut für Agrarforschung INRA Bordeaux, die Softwareschmiede ESI Group und der Wetterdienst Meteo France sowie das Schweizer Startup-Unternehmen Sorim.

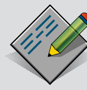


Suns Rekord im Java-Business-Benchmark

Die Bestmarke für Java-getriebene x86-Server reklamiert Sun Microsystems für sich: 683 542 Business Operations per Second (bops) und 85 443 bops pro Java Virtual Machine (JVM) hat der Fire X4600 M2 im JBB2005 erzielt, wobei Sun seine JVM Hotspot 1.6 in einer Performance Release einsetzt. Der 4U hohe Rechner läuft mit acht Opterons vom Typ 8360SE (Barcelona) unter Solaris 10.



KURZ NOTIERT



Mainframe im Browser: Um auf IBMs System z per Browser zugreifen zu können, hat Compuware die Software Abend-AID entwickelt. Mit der neuen Version 11 können Mitarbeiter leichter als über das Kommando-Interface Fehleranalysen in Cobol- und Assembler-Programmen durchführen (www.compuware.com).

HPC-Probe: The Partnership for Advanced Computing in Europe (PRACE) hat einen Prototyp des Roadrunner erhalten. Er steht im Supercomputer Center Barcelona (www.bsc.es), der Heimat des spanische Superrechners Mare Nostrum. Die Maricel-Initiative, die bei der Auswahl von Hard- und Software maßgeblich beteiligt ist, will den HPC-Rechner unter die Lupe nehmen (www.prace-project.eu).

WLAN embedded: Global Edge Software und QNX kooperieren. Sie haben in QNX’ Neutrino RTOS einen WLAN/WiFi-Treiber für Marvell-Chips integriert. Es gibt ihn sowohl für den Netzwerkstack *io-net* als auch für den neuen *io-pkt*.

Im Kasten: In einem 12 m langen Container bringt Hewlett-Packard ein Rechenzentrum unter. Binnen sechs Wochen nach Auftragseingang soll es beim Kunden stehen. Das Performance Optimized Data Center (www.hp.com/go/pod) bietet laut HP Platz für mehr als 3500 Rechnerknoten und über 12 000 Festplatten im 3,5-Zoll-Format.

QNX’ freie Quellen zum Dritten

Unter der Lizenz „QNX Hybrid Software Model“ hat QNX nach den Quellen des Microkernel Neutrino und des Network Stacks *io-pkt* nun auch die der Dateisysteme des Echtzeitbetriebssystems RTOS Neutrino freigegeben. Die Software gibt es zum freien Download, Lizenzgebühren fallen erst beim kommerziellen Einsatz in Produkten an. Die dem POSIX-Standard folgenden Filesysteme enthalten Schnittstellen für Festplatten (SCSI, IDE, SATA), CD/DVD-Laufwerke, USB-Sticks, RAM-Disks und fest eingebaute NAND/NOR-Flash-Chips. Außerdem unterstützen sie NFS (v2, v3) sowie CIFS für den Netzwerkzugriff. Über FAT lassen sich Daten mit Windows austauschen und über EXT2 mit der Linuxwelt. Hinzu kommen zwei Dateisysteme für Flash Chips, das Embedded Transaction File System (ETFS) für NAND- und das Flash File System (FFS3) für NOR-Flash.

ETFS ist gegen Datenverlust bei Stromausfall geschützt und nutzt zur Fehlerkorrektur CRC und ECC. Zu den besonderen Merkmalen gehört die automatische Defragmentierung. Hinzu kommen weiter Techniken zum Schutz der Chips und der Daten, darunter dynamisches und statisches Wear Leveling und Read Degradation Monitoring. FFS3 beherrscht Wear-Leveling, Error Handling, Background Reclaim, Fault Recovery, transparente Dekomprimierung, Multithreading sowie Endian Awareness. Große Festplatten schützt bei einem Stromausfall laut QNX das Power-Safe File System. Es verwendet die Copy-on-Write-Technik, die vor allem zeitraubende Integrity-Checks vermeiden hilft.

Embedded-Entwickler erhalten bei QNX Zugriff auf Code-Updates, Bug-Fixes und Produktentwicklungen. Außerdem gibt es die Entwicklungsumgebung QNX Momentics kostenlos per Download zum Test.

Axel Urbanski



AMD überarbeitet Stream SDK

Vor allem an der Unterstützung von DirectX 11 und OpenCL arbeitet das Entwicklerteam des Stream SDK bei AMD/ATI (ati.amd.com). Es dient dazu, Anwendungen zu erstellen, die von den Hunderten Cores in den Grafikprozessoren (GPUs) profitieren. Das Stream SDK soll vor allem das Erstellen von Applikationen für General-Purpose-GPUs (GPGPUS) vereinfachen. AMD will durch sein Engagement OpenCL als Standard etablieren. Die Open Computing Language mit einer C-ähnlichen Syntax generiert eine Run-Time-Umgebung, die Programme zur Laufzeit auf CPUs und GPUs verteilt.



Bull will Petaflop-Rechner bauen

Zur Simulation von Atomwaffen entwickeln Bull und die Abteilung für militärische Anwendungen (DAM) der französischen Atomenergiebehörde (CEA) gemeinsam einen Supercomputer, der mehrere Petaflop/s (Billionen Flop/s) erreichen soll.

Bei dem geplanten Tera 100 – Nachfolger des Linux-Clusters Tera 10 (Rang 32 in den Top500) – will man statt der bisherigen Itanium2-CPUs von Intel eine x86-Architektur verwenden.

iX-Link ix0809020



In der Kritik

Die derzeitigen Pläne der Bundesregierung zur erleichterten Zuwanderung ausländischer Fachkräfte gehen dem Bitkom nicht weit genug. „Die Maßnahmen der Bundesregierung werden kaum einen Beitrag zur Linderung des Expertenmangels leisten können“, lässt sich August-Wilhelm Scheer, Präsident des ITK-Lobbyverbandes, zitieren. Die neue Regelung sieht eine Reduzierung der Jahresverdienstgrenze von bisher 86 400 € auf 63 600 € vor. Scheer zufolge verhindert aber eine Gehaltsgrenze über 45 000 € den Zuzug der besonders mobilen Absolventen ausländischer Hochschulen. Positiv bewertet wird dagegen, dass künftig Zuwanderer, die zwei Jahre in ihrem Beruf gearbeitet haben, dauerhaft in Deutschland bleiben dürfen. Dies eröffne ausländischen Hochschulabsolventen, die in Deutschland ihren Abschluss gemacht und anschließend hier einen Job gefunden haben, endlich eine sichere Perspektive.

Interkultureller Aufbau für Masterstudiengang

An der Hochschule Amberg-Weiden startet zum Wintersemester 2008/2009 mit „Interkulturelles Unternehmens- und Technologiemanagement“ ein neuer Masterstudiengang. Das Studium erfolgt in Kooperation mit der Hochschule Regensburg, der Wirtschaftsuniversität Prag und dem Europaeum der Universität Regensburg. Es vermittelt – aufbauend auf einem Erststudium in den Ingenieur- oder Wirtschaftswissenschaften – Kompetenzen für Führungskräfte in einem interkulturellen und technologiegeprägten Umfeld. Das soll helfen, technische Entwicklungen und deren Bedeutung, betriebs- und volkswirtschaftliche Zusammenhänge sowie die Bedeutung kultureller Faktoren in der internationalen Dimension zu verstehen und dieses Wissen in der betriebliche Praxis umzusetzen. Mit dem Abschluss wird der akademische Grad eines „Master of Arts“ verliehen. Weitere Infos unter www.haw-aw.de.

KURZ NOTIERT

Interdisziplinär: Mit dem WS 08/09 startet an der RWTH Aachen der Bachelorstudiengang Technik-Kommunikation, ab dem WS 10/11 folgt ein Masterstudiengang. Das Studium Technik-Kommunikation verbindet die Kommunikationswissenschaft mit technischen Fächern wie Elektrotechnik, Informatik und Maschinenbau. Infos unter www.tk.rwth-aachen.de.

Standortfrage: Das auf Vergütungsthemen spezialisierte Beratungsunternehmen Personalmarkt hat mehr als 100 000 aktuelle Gehaltsdaten aus deutschen Großstädten ausgewertet und in ein Ranking gebracht. Demnach liegt das Gehaltsniveau in Frankfurt um 18 %, in München um 15 % höher als der Bundesdurchschnitt, in Dresden und Leipzig dagegen um 11 % und 17 % unter dem Durchschnitt.

KDE 4.1 für Anwender

Drachenfeuer

Susanne Nolte

Mit KDE 4 wollen die Entwickler der freien Desktop-Umgebung zu Mac OS X und Vista aufschließen – und gleichzeitig neue Welten erobern. Nun ist mit KDE 4.1 die erste stabile Version erschienen.

Ende Juli haben die KDE-Entwickler die Version 4.1 freigegeben. Nachdem das Anfang 2008 veröffentlichte KDE 4.0 nur für Entwickler gedacht war, soll die zweite Version der KDE-4-Entwicklungsreihe die Anwender-Desktops schmücken. Dafür wartet sie mit neuen Programmbibliotheken wie Qt 4.4, erweiterter Unterstützung für andere Plattformen, der ausgewachsenen Arbeitsoberfläche Plasma sowie neuen Funktionen und Anwendungen auf.

Mit dem Umstieg auf Qt 4.4, deren neue Widgets vor allem der mit KDE 4.0 eingeführten Arbeitsoberfläche Plasma zugutekamen, können die Entwickler direkt auf die ebenfalls enthaltene HTML-Rendering-Engine Webkit zugreifen, etwa um Dashboard-Widgets von Mac OS X einzubinden. Außerdem verbessert das neue Multimediasystem Phonon mit zusätzlichen Backends für GStreamer, Quicktime und Directshow 9 die Multimedia-Unterstützung auf Windows und Mac OS. Nichtsdestotrotz ist KDE on Mac (mac.kde.org) noch nicht bereit für den produktiven Einsatz, auch die Integration von Hardware und Suchfunktion fehlt noch.

Für Windows-Entwickler existieren hingegen Vorabversionen von KDE-Anwendungen zum Herunterladen (windows.kde.org). Die Entwickler beschreiben die Bibliotheken für KDE on Windows als relativ stabil, doch sind noch nicht alle Funktionen der *kdelibs* verfügbar. Zudem bringen die Entwickler gerade die Open-Solaris-Unterstützung von KDE in Form und beheben einige Stolperfallen (techbase.kde.org/Projects/KDE_on_Solaris).

Wieder auferstanden ist das Personal Information Management PIM, das unter anderem das E-Mail-Programm KMail, den Kalender KOrganizer, den RSS-Feedreader Akregator und den Newsgroup-Reader KNode in die Kontact-Oberfläche integriert. Das PIM-Datenhaltungs-Framework Akonadi vereinfacht das Empfangen und Speichern von E-Mails und Kontaktdaten über Anwendungsgrenzen hinweg. Es verwaltet sowohl Daten als auch Datenquellen und informiert Anwendungen über Änderungen. Bisher greift aber einzig das IMAP-E-Mail-Programm Mailody auf den Akonadi-Server zu.

Die Schnittstellen für Python und Ruby sollen inzwischen so ausgereift und stabil sein, dass sich KDE-Anwendungen in diesen Sprachen schreiben lassen. Auch die Bibliothek *libksane* ist überarbeitet und soll den Zugriff auf Scan-Programme wie das neue Skanlite vereinfachen. Hinzu gesellt sich ein gemeinsames Emoticon-System, das KMail und Kopete bereits nutzen.

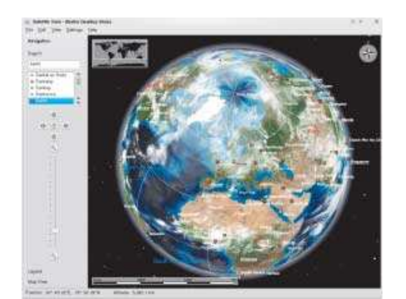
Neu ist der Hex-Editor Okteta. Nicht mehr ganz so neu ist der überarbeitete Video-Player Dragon, der unter KDE 3 noch Codeine hieß. Auch den CD-Spieler KSCD haben die Entwickler wiederbelebt.

KDEs junger Dateiverwalter Dolphin hat Tabs sowie eine Baumansicht in der Hauptansicht bekommen. Sein Vorgänger Konqueror, der nun vor allem als Internet-Browser dient, kann jetzt bereits geschlossene Fenster und Tabs wieder öffnen. Der Bildbetrachter Gwenview hat unter anderem eine neue Vollbildansicht und ein Undo-System bekommen.

KRDC, KDEs Client für entfernte Desktops, kann nun über das Zeroconf-Protokoll (alias Rendezvous, bestehend aus Multicast DNS und DNS Service Discovery) entfernte Rechner im lokalen Netz automatisch entdecken. In den virtuellen Globus Marble, den die Entwickler mit KDE 4.0.3 nachgereicht hatten, haben sie mittlerweile eine Schnittstelle zum Open-Street-Map-Projekt (www.openstreetmap.org) integriert. Auf Hardwarebeschleunigung – etwa OpenGL – haben sie jedoch verzichtet, damit Marble auch auf älteren Rechnern läuft. KWin, der Fensterverwalter von KDE, hat ebenfalls Erweiterungen wie Cover-Wechsel und „wackelige“ Fenster (wobbly windows) erfahren.

Eine schlechte Nachricht gibt es für Benutzer von Nvidia-Karten, die den proprietären *nvidia*-Treiber installiert haben. Sie müssen mit Geschwindigkeitseinbußen beim Wechseln und Vergrößern oder Verkleinern von Fenstern rechnen. Vorläufige Workarounds sind in der Techbase zu finden (techbase.kde.org/User:Lemma/GPU-Performance). (sun)

iX-Link ix0809022



An Google Earth erinnert der freie, virtuelle Globus Marble (links). Über die Integration von Open Street Map lässt sich das bisher verfügbare Material der Free Wiki World Map abrufen (rechts).

Snapshot-Dateisystem Tux3 angekündigt

Nach mehrjähriger Pause hat Daniel Phillips eine komplett überarbeitete Version 3 seines Dateisystems Tux angekündigt. Auszeichnen soll es sich vor allem durch eine effiziente Versionierung (Snapshots) und die Remote-Replikation von Dateien, Verzeichnissen oder des gesamten Filesystems. Ebenfalls geplant sind eine Fragmentierungskontrolle, in der Größe variable und dynamisch allozierbare Inodes, eine neue atomare Update-Methode, genannt Forward Logging, ein physisch stabilerer Verzeichnisindex (PHTree) und BTree-Backpointer für ein robustes *fsck*. Zudem sollen alle Snapshots schreibbar sein.

Die maximale Datei- und Volume-Größe soll 1 Exabyte (2^{60} Byte) betragen; die maximale Zahl der Inodes beträgt 2^{48}. Im Gegensatz zum Standard-Dateisystem ext3fs arbeitet Tux3 nicht mit Blöcken fester Größe, sondern mit zusammenhängenden Speicherbereichen beliebiger Größe (Extents). Die neue Versionierungsmethode (Versioned Pointers) soll sowohl Daten als auch Metadaten umfassen.

Vor zehn Jahren hatte Phillips den Prototyp von Tux2 für den Linux-Kernel 2.2.13. entwickelt. Da der Code aber an mindestens drei Stellen bestehende Patente verletzte, durfte Phillips ihn nie veröffentlichen. Die Ankündigung mit einer detaillierten Beschreibung von Tux3 findet sich auf der Linux Kernel Mailingliste (article.gmane.org/gmane.linux.file-systems/24998) und auf tux3.org/design.html.



Mehr Urheberschutz bedeutet weniger Datenschutz

Am 1. September 2008 tritt das „Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ in Kraft. Mit mehr als zwei Jahren Verspätung hat Deutschland damit die sogenannte „Enforcement-Richtlinie“ der Europäischen Union in nationales Recht umgesetzt. Interessant sind im Wesentlichen zwei Regelungen des Gesetzes: der Auskunftsanspruch über Rechtsverletzer und die Deckelung von Abmahnkosten in bestimmten Fällen.

Verletzt jemand in „gewerblichem Ausmaß“ Rechte Dritter, beispielsweise Urheberrechte, hat der Geschädigte einen Auskunftsanspruch insbesondere gegen Internetprovider über die Identität des Rechtsverletzers, damit er gegen diesen rechtlich vorgehen kann. Was „gewerbliches Ausmaß“ im Einzelfall bedeuten soll, entscheiden letztlich die Gerichte. Immerhin soll nach dem Willen des Gesetzgebers nicht allein die Anzahl etwaiger Uploads entscheiden, sondern es kann auch eine besonders umfangreiche Datei den Auskunftsanspruch begründen. Wenn die Provider zur Auskunftserteilung auf dynamische IP-Adressen (oder andere „Verkehrsdaten“) zugreifen müssen, muss dem aber vorab ein Richter zustimmen.

Bei einfach gelagerten Fällen von Urheberrechtsverletzungen im nichtgewerblichen Bereich sind Abmahnkosten nun auf 100 Euro gedeckelt. Das soll dem Unwesen der Massenabmahnungen von Verbrauchern Einhalt gebieten. Auch mit dieser Neuregelung werden sich Gerichte beschäftigen müssen, um den Anwendungsbereich im Detail auszuleuchten. *Tobias Haar*



Gebührendeckel: Ein Gesetzesentwurf sieht vor, dass künftig Anrufe bei 0180-Nummern aus dem Mobilfunknetz höchstens 28 Cent pro Minute oder 40 Cent pro Anruf kosten dürfen.

Verbraucherschutz: Die Bundesregierung plant eine Änderung des Bundesdatenschutzgesetzes wegen des umstrittenen Schuldner-Scoring. Die neuen Verbraucherschutzvorschriften stehen ab kommendem Herbst zur Bundestagsdebatte an.

Schutz vor Telefonwerbung: Das Bundeskabinett hat ein Gesetz auf den Weg gebracht, das bei telefonisch abgeschlossenen Verträgen eine 14-tägige Widerrufsmöglichkeit vorsieht.

Meldepflicht: Der Bundesbeauftragte für den Datenschutz, Peter Schaar, hat eine Meldepflicht nach US-amerikanischem Vorbild für Fälle des Datenmissbrauchs gefordert. In den USA haben bereits 44 Bundesstaaten solche Pflichten eingeführt.

GEZ-Gebührenpflicht für Firmen-PCs vor Gericht

Nach der Einführung einer Rundfunkgebühr für sogenannte „neuartige Rundfunkgeräte“ ab dem 1. Januar 2007 gibt es nun die ersten Gerichtsentscheidungen zu Grenzfällen. Das Verwaltungsgericht Braunschweig hat kürzlich entschieden, dass die GEZ für den beruflich genutzten PC in einem in der eigenen Wohnung liegenden Arbeitszimmer diese Gebühr nicht festsetzen und einziehen darf (Az. 4 A 149/07). Die Richter schlossen sich der Auffassung des „Gebührenschuldners“ an, dass ein beruflich genutzter PC als Zweitgerät von der Gebühr in Höhe von 5,52 Euro pro Monat befreit ist, wenn in dieser Wohnung weitere regulär angemeldete Empfangsgeräte vorhanden sind. Das regelt der Rundfunkgebührenstaatsvertrag: „Für neuartige Rundfunkempfangsgeräte im nicht ausschließlich privaten Bereich ist keine Rundfunkgebühr zu entrichten, wenn […] andere Rundfunkempfangsgeräte dort zum Empfang bereitgehalten werden.“

In einem anderen Fall hatte das Verwaltungsgericht Koblenz entschieden, dass für den PC in einer Anwaltskanzlei, der für Datenbankrecherchen sowie für Steuererklärungen dient, ebenfalls keine solche Gebühr fällig wird (Az. 1 K 496/08.KO). Es reicht nicht, dass eine „abstrakte technische Möglichkeit des Rundfunkempfangs“ besteht. Der PC muss zusätzlich „zum Empfang“ bereitgehalten werden. Dies ist aber nicht der Fall, da in der Kanzlei des Anwalts typischerweise keine Rundfunknutzung stattfindet. Beide Urteile sind noch nicht rechtskräftig, das letzte Wort ist also noch nicht gesprochen. *Tobias Haar*

Keine SMS-Werbung ohne Zustimmung

Der Bundesgerichtshof hat Payback eine schwere juristische Niederlage bereitet. Ohne vorherige Zustimmung der Adressaten ist das Versenden von E-Mail oder SMS rechtswidrig. Bisher erhielt jeder Payback-Kunde elektronische Werbung, wenn er nicht aktiv widersprochen hatte. In den allgemeinen Geschäftsbedingungen hatte Payback vorgesehen, Kundendaten für Zwecke der Werbung und Marktforschung zu verwenden. Diese Klausel bedeutet nach Ansicht der BGH-Richter eine „unzumutbare Belästigung“ für Verbraucher und sei nach den Regeln des Rechts der allgemeinen Geschäftsbedingungen unwirksam.

Bedeutsam ist, dass die Kunden dieser Form der Datennutzung aktiv hätten widersprechen müssen. Die Payback-AGB sahen folgende Wahlmöglichkeit vor: „Hier ankreuzen, falls die Einwilligung nicht erteilt wird.“ Deutschem Recht genügen solche Opt-out-Konstruktionen jedoch nicht. Nur wenn Kunden aktiv der Datennutzung zustimmen (Opt-in-Verfahren), sind Einwilligungen rechtswirksam. Für Werbung per Post allerdings hat der BGH dieses Verfahren zum wiederholten Male als zulässig angesehen. *Tobias Haar*

KURZ NOTIERT

Endpoint-Security: Das Upgrade von Symantecs Network Access Control gewährleistet nicht nur die Durchsetzung von Sicherheitsrichtlinien und überprüft den Compliance-Status von Endgeräten, sondern bietet einen On-Demand-Client an. Mit ihm können Gastbenutzer nach einer Reihe vorgegebener Sicherheitsprüfungen auf das Netzwerk zugreifen.

Schutz gegen „Pump and Dump“: Einen Echtzeitschutz gegen Aktienbetrug, bei dem die Betrüger Aktien via Phishing-Mail erst puschen, dann abstoßen, bietet Verisign (www.verisign.com) für Kreditinstitute und Börsenhändler. Dazu untersucht ein Fraud-Detection-Modul Aktientransaktionen sowohl regel- als auch verhaltensbasiert und informiert Kunden über Unregelmäßigkeiten.

Device-Kontrolle: In der neuen Version 4.3 schützt die Sicherheitssoftware für mobile Speichergeräte Sanctuary von Lumension Security (www.lumension.com) auch CDs und DVDs vor unbefugtem Zugriff. Das Produkt soll durch die per Policy durchsetzbare Verschlüsselung von PGP außerdem das Abfließen vertraulicher Daten verhindern.

Online-Backup: Speziell für den Mittelstand bietet Black Point Arts seine Online-Backup-Dienste an (www.back2web.de). Die Daten werden mit 256 AES verschlüsselt und im Rechenzentrum von Black Point Arts in Frankfurt automatisiert gesichert. Zur Verfügung stehen der Back2Web-Secure-Client-Account für 2,99 € pro Monat plus 0,39 € je GByte Daten sowie der Back2Web-Secure-Server-Account für 4,99 € pro Monat plus 1,19 € pro GByte.

iX-Link ix0809026

Microsoft: Schwachstellen früher bekannt geben

Einen weiteren Vorstoß in Sachen Sicherheit macht Microsoft mit zwei neuen Initiativen, die das Unternehmen auf der diesjährigen Black Hat (s. S. 12) vorstellte. Im Rahmen des Microsoft Active Protections Program (MAPP) will es, schon bevor die monatlichen Sicherheits-Updates erscheinen, relevante Informationen zu Schwachstellen und Schadcode an Hersteller von Sicherheitssoftware übermitteln. So können diese ihre Produkte schneller an die Bedrohungen anpassen. Damit Anwender die Gefährdung ihrer Systeme besser einschätzen können, soll es zukünftig auch einen Exploitability Index geben. Dieser drückt aus, wie hoch die Wahrscheinlichkeit ist, dass Cyberkriminelle für eine Sicherheitslücke ein Angriffsprogramm (Exploit) schreiben. Entsprechend können Anwender Prioritäten beim Aktualisieren oder Patchen ihrer Systeme festlegen. Kurze Zeit nach der Black Hat kündigte das Unternehmen außerdem sein Microsoft Vulnerability Research Program (MSVR) an. Zukünftig wolle man Windows-Anwendungen von Drittanbietern sicherer machen und die Hersteller mit Informationen und Lösungsansätzen aktiv dabei unterstützen.

SPIT-Testsoftware für VoIP-Anlagen

Bei der SPIT-Bekämpfung helfen Gegenmaßnahmen aus dem Spam-Umfeld nicht. Um SPIT (Spam over Internet Telephony) besser abwehren zu können, haben Forscher am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) eine Simulationssoftware entwickelt, mit der Administratoren ihre VoIP-Anlagen testen können. SIP XML Scenario Maker (SXSM) versendet SPIT-Testanrufe an die eigene Anlage und speichert die Rückmeldungen in auswertbaren Tabellen.

Die Forscher demonstrieren zum Beispiel, dass Spitter die Telefonnummern der VoIP-Accounts gar nicht kennen müssen, sondern leicht durch Ausprobieren ermitteln können. Erste Versuche hätten gezeigt, dass alle Typen von VoIP-Anlagen von der SPIT-Gefahr betroffen sind. Weitere Infos enthält die Studie „SPAM over Internet Telephony and how to deal with it“ (s. *iX*-Link). Die Software basiert auf dem frei verfügbaren Open-Source-Testwerkzeug SIPp. Interessierte können es über das Fraunhofer-Institut bekommen. Den Quellcode des SXSM-Werkzeugs gibt es hier: code.google.com/p/sxsm. *Barbara Lange*



RFID-Pausensteuerung für Callcenter

Die Voxtron GmbH (www.voxtron.de) hat die Funktionen ihrer Contact-Center-Software agenTel erweitert. Sie bündelt E-Mails und Telefonate unter einer Oberfläche und leitet sie an den fachlich am besten geeigneten oder verfügbaren Mitarbeiter weiter. Wenn dieser aber gerade nicht an seinem Arbeitsplatz ist, sollten die Anrufe nicht ins Leere laufen. Diesen Prozess soll das neue Modul „AutoPause“ gewährleisten und automatisieren. Das Modul besteht aus einem Transponder, einem USB-Dongle und einem Software-Plug-in.

Den RFID-Transponder trägt der Callcenter-Agent bei sich. Entfernt er sich länger als 30 Sekunden mehr als 2 Meter von seinem Rechner, bekommt das Software-Plug-in dies über den USB-Dongle mitgeteilt, sperrt den Rechner und leitet eingehende Anrufe an andere Mitarbeiter weiter. Die Freigabe erfolgt automatisch bei der Rückkehr des Agenten. Als Vorteile nennt der Hersteller eine bessere statistische Auswertung und den Wegfall von Passwörtern. Das Modul „AutoPause“ ist ab sofort erhältlich. Datenschutzkollisionen sieht das Unternehmen nicht, denn diese hängen nicht vom Modul, sondern von der Konfiguration (beispielsweise ob ein personenbezogenes Logging stattfindet oder nicht etc.) ab. *Barbara Lange*

Netzwerkscanner für Unternehmen

Eine kompakte und einfach zu konfigurierende Scan-Appliance für Unternehmen ohne eigene IT-Sicherheitsabteilung bringt der amerikanische Hersteller eEye Digital Security (www.eeye.com) auf den Markt. Die Retina Appliance 651 enthält einen Network Security Scanner für die Schwachstellensuche, den Network Traffic Analyzer zum Entdecken verdächtiger Datenströme sowie ein hostbasiertes Intrusion-Prevention-System. Für das Scannen nach Schwachstellen ist ein Client mit Remote Desktop erforderlich. Über ihn kann der Verantwortliche die Appliance konfigurieren und bedienen. Gesonderte Eingabe-Hardware ist nicht erforderlich, die Retina Appliance bringt ein LC-Display nebst Eingabefeld mit. Das Gerät ist ab sofort erhältlich, eine Appliance für 128 Systeme kostet 2585 €.



PDF-Tools mit neuem PDF/A-Konverter

Auf der diesjährigen DMS will die Schweizer PDF Tools AG ihren neuen 3-Heights Document Converter Service vorstellen. Dieses Produkt wandelt E-Mails mitsamt ihren Anhängen in eine einzige PDF/A-Datei um, die auch nach zwanzig Jahren noch lesbar sein soll. Alle MS-Office-Dateien, PDFs und gängige Bildformate konvertiert das Werkzeug ebenfalls in das Langzeitarchivierungsformat. Eine digitale Signatur soll Rechtssicherheit gewährleisten. Via Programmierschnittstelle lässt sich der Service in bestehende Anwendungen integrieren (www.pdf-tools.com).

IBM: Archivierung für SAP-Daten

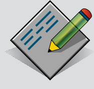
Eine Komplettlösung aus Hard- und Software für Daten- und Dokumentenarchivierung in SAP-Systemen bietet IBM an. Die Offerte richtet sich speziell an kleine und mittlere Unternehmen. Das Paket umfasst die Commonstore-Archivierungssoftware, den Server X3650 sowie das DR550-Plattenspeichersystem für die gesetzeskonforme Datenaufbewahrung. Bis zum 31. Dezember 2008 können Interessierte das Bundle ab 23 862 Euro erwerben. Es ist für typische Konfigurationen mit 100, 250, 500 und 1000 Anwendern verfügbar und lässt sich durch zusätzliche Lizenzen ausbauen.

SAS verstärkt sich mit Ideas

SAS hat den US-amerikanischen Anbieter von Revenue-Management-Produkten Ideas übernommen, der zahlreiche Unternehmen aus der Tourismusbranche zu seinen Kunden zählt, darunter viele große Hotelketten. Diese Softwaregattung, die Ideas im Mietmodus anbietet, soll Kundenverhalten vorhersagen und die Preisgestaltung optimieren. So können Hotels beispielsweise an umsatzschwachen Tagen spezielle Angebote machen. SAS ergänzt mit Ideas Palette seine Ertragsoptimierungslösung für den Handel. Man will die Produkte in die eigene BI-Plattform einbinden und auf die Bedürfnisse weiterer Branchen zuschneiden. Ideas wird als hundertprozentige Tochter von SAS weitergeführt. Den Kaufpreis gab man nicht bekannt.



KURZ NOTIERT



Alfresco auf Ubuntu: Ubuntu-Sponsor Canonical stellten ein Bundle aus dem Linux-Betriebssystem sowie dem CMS Alfrescos Labs 3 (Beta) vor. Canonical will die Software als vorkonfiguriertes und getestetes Produkt noch in diesem Jahr anbieten. Dann soll auch das CMS den finalen Status erreicht haben. Eine Version mit professionellem Support ist ebenfalls noch für dieses Jahr geplant.

BPM unter der Lupe: In der Studie „Business Process Management Tools 2008“ stellt das Fraunhofer IAO 18 entsprechende Werkzeuge vor. Die betrachteten Merkmale sollen sich an den Anforderungen typischer Einsatzszenarien orientieren. Die Untersuchung kostet 200 Euro und ist über den IAO-Shop zu beziehen: www.iao.fraunhofer.de/d/shop.

Besser geregelt: Das Softwarehaus Innovations hat die Version 4.2 des Business-Rules-Managementsystems Visual Rules freigegeben. Es arbeitet mit der Eclipse-Plattform 3.4. zusammen. Beispielsweise lassen sich jetzt Abhängigkeiten zwischen Regeln und Modellen grafisch darstellen sowie Regelstatistiken aus Produktions- und Testumgebungen importieren.

ECMS Alfresco als Sharepoint-Alternative

Unter dem Namen Alfresco Labs 3 haben die Entwickler des Enterprise-Content-Mangement-Systems Alfresco eine Betaversion ihres Open-Source-Produkts vorgestellt, das eine Alternative zu Microsofts Sharepoint sein soll (wiki.alfresco.com/wiki/Alfresco_Labs_3). Nach Angaben von John Newton, einem der Mitgründer des mittlerweile bei EMC angesiedelten Documentum, handelt es sich um die erste Open-Source-Alternative zu Sharepoint. Voraussetzung für die Entwicklung war, dass Microsoft sein Sharepoint-Protokoll veröffentlicht hatte.

Anwender von Microsofts Office-Produkten sollen aus diesen heraus auf das Alfresco-Repository zugreifen können, ohne einen Unterschied zu bemerken. Mit der im Gesamtpaket oder als eigenständiges WAR-Archiv installierbaren Plattform enthält Alfresco3 eine Webanwendungsumgebung (Surf), die beispielsweise die Verwendung von Java, JSP, HTML, serverseitigem Javascript und der Freemarker-Template-Engine erlaubt. Surf nutzt Yahoos UI-Bibliothek und Adobes Flex, um Daten zu laden und Inhalt als Vorschau zu zeigen. Die Betaversion ist sofort freigegeben. Als Enterprise-Produkt soll Alfresco 3 im Oktober auf den Markt kommen.

iX-Link ix0809028

Optimiertes LAMP für Solaris und Linux

Als Sun Web Stack (früher: Cool Stack) hat Sun Microsystems sein Open-Source-Paket mit Support für Unternehmen vorgestellt. Das von Sun AMP (Apache, MySQL, PHP/Perl) genannte Bündel soll im dritten Quartal für Solaris und im vierten für Linux vorliegen. Windows und weitere Systeme sollen folgen. Zum Web Stack gehören Apache 2.2.8, MySQL 5.1, PHP 5.2.5, Ruby 1.8.6, Perl 5.8.8, Tomcat 6.0.16 und Squid Proxy 2.16.x. Den Quellcode für den Java System Web Server 7.0 will Sun im Laufe des dritten Quartals 2008 unter einer BSD-Lizenz zur Verfügung stellen.

EMCs Documentum 6.5: Neue Clients

Seit Ende Juli soll Version 6.5 von EMCs DMS/CMS Documentum erhältlich sein – bis auf die zwei neuen Clients Centerstage Essentials und My Documentum. Die beiden Clients, so EMC, kommen im dritten Quartal dazu. Außerdem hat EMC das XML-DBMS Xhive der im vorigen Jahr übernommenen gleichnamigen Firma integriert, sodass Documentum jetzt durchgängig XML unterstützt. Centerstage Essentials ist ein Client für die Arbeit mit Documentum. My Documentum kommt als Offline-Client hinzu, sodass Anwender ohne Server-Zugriff arbeiten können. Außerdem enthält die Software einen auf Adobes Flex aufsetzenden Editor für das Web Content Management sowie einen Client für die Verwaltung multimedialer Inhalte.

KURZ NOTIERT

Google-Einsicht: Unter dem Namen Google Insights for Search können Suchbegriffe und Regionen oder Städte in Beziehung gesetzt werden (www.google.com/insights/search/).

Onlinebuchhandel: Ende des Jahres will Amazon den auch in Deutschland tätigen Onlinebuchhändler Abebooks (www.abebooks.de) übernehmen, der vor allem im antiquarischen Bereich arbeitet.

Wolkensuche: Searchcloud ist der Name einer neuen Suchmaschine, die es Nutzern erlaubt, einzelne Suchbegriffe unterschiedlich zu gewichten (www.searchcloud.net).

Cuil will Google Konkurrenz machen

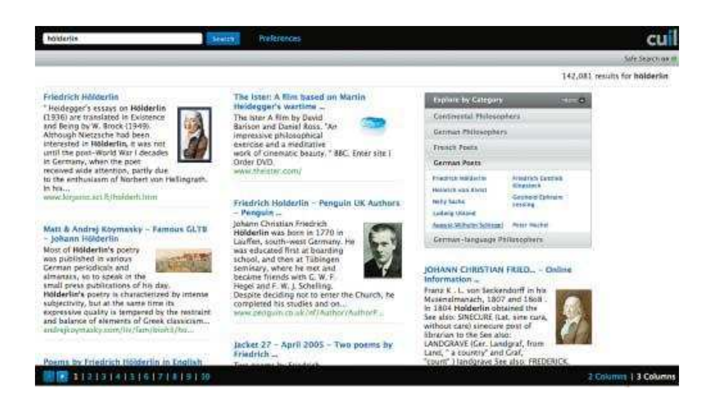
Mit dem Anspruch „Biggest Search Engine on the Web“ kündigte die im kalifornischen Menlo Park ansässige Cuil (www.cuil.com) Ende Juli ihre neue Suchmaschine an, die nach eigenen Angaben mit 120 Milliarden Websites dreimal so viel wie die Konkurrenz durchsucht. Der gälische Name, wie das englische „cool“ auszusprechen, bedeutet so viel wie Wissen. Gegründet haben Cuil ein Ex-IBM-Manager und drei ehemalige Google-Mitarbeiter. An Venture-Kapital soll es nicht mangeln.

Clou der neuen Suchmaschine: Anders als Google erhebt und speichert Cuil keine Nutzerdaten. Und die dreispaltige Darstellung (siehe Screenshot) samt den rechts zu sehenden aufklappbaren Kategorien verspricht mehr Übersicht.

Momentan konzentriert Cuil sich auf die englische Sprache, bei deutschen Informationen kann sie nicht mit Google mithalten. Die im Grunde gute Idee, gefundenen Seiten gleich ein Bild mitzugeben, führen die Cuiler allerdings ad absurdum, wenn Bild und Text nicht zueinander passen, wie im Screenshot in der Mitte (Trakl beim Hölderlin-Link).

Ein Suchbeispiel mit US-Bezug („edgar allan poe“) ergab für Cuil gute 2,6 Millionen Treffer, Google brachte es dagegen auf 5,5, wobei einige Ergebnisse bei beiden identisch waren, Google deutschsprachige Seiten einbezog und Cuil einen falschen Kalenderlink bei Wikipedia referenzierte. Erst mittelfristig dürfte sich zeigen, ob die inhaltsorientierte Suche gegen das Page Ranking eine ernsthafte Chance hat.

iX-Link ix0809028



Apache bringt neue FOP-Version

Ein Jahr nach der letzten Release gibt die Apache Foundation Version 0.95 ihres Formatting Objects Processor (FOP, xmlgraphics.apache.org/fop/) frei. Damit entfällt die Unterstützung für Java 1.3, ab jetzt ist mindestens 1.4 erforderlich. Verbessert haben die Entwickler den Release Notes zufolge die Behandlung von Tabellen: Der Prozessor interpretiere nun sowohl *keep*-Attribute, mit denen sich die Tabelle mit vorangehendem oder folgendem Text auf einer Seite halten lässt, als auch die *break*-Eigenschaften, die vor oder nach der Tabelle einen Seitenumbruch erzwingen. Für Spalten lässt sich ebenso wie für die Überschrift und die Fußzeilen eine Hintergrundfarbe angeben. Insgesamt sei Apache FOP schneller geworden und habe weniger Fehler. Eine komplette Liste der Änderungen ist online verfügbar.

Apache FOP ist ein XSL-Prozessor, der XML-Dokumente für die Druckausgabe aufbereitet. Er kann unter anderem PDF, Postscript, die von HP entwickelte Druckersprache PCL sowie RTF (Rich Text Format) erzeugen. Das für Archivierungszwecke verwendete PDF/A unterstützt er jedoch noch nicht vollständig. Die Software ist in Java geschrieben und steht unter der Apache-Lizenz. Sie lässt sich von den Projektseiten herunterladen.

iX-Link ix0809028

Erste FCoE-HBAs

Converged Network Adapter (CNAs) heißen die Einbauplatinen für Fibre Channel over Ethernet (FCoE). Ihrer zwei hat QLogic nun auf den Markt gebracht. Der QLE8042-CK besitzt zwei Ports für Twisted Pair-Kabel (max. 10 m), der QLE8042-SR-CK zwei LWL-Ports (300 m). Beide benötigen sowohl PCIe-x8-Slots als auch 10-Gigabit-Ethernet. Sie besitzen eine Engine für TCP/IP-Checksum- sowie Large Send Offload (LSO) und unterstützen Jumbo-Frames (9,6 kByte).

Treiber existieren für Windows 2003 und 2008, Red Hat AS 4/5 sowie SLES 10 (32- und 64-Bit-x86). QLogic bietet die CNAs auch zusammen mit den Cisco-Switches Nexus 5000 als FCoE-Paket an.

Bereits im April hatte Intel neue Treiber angekündigt, die die 10-Gigabit-Ethernet-Server-HBAs um FCoE erweitern. Die für Juli versprochenen RHEL-Treiber lassen allerdings ebenso auf sich warten wie die für Windows.

RAM im SAN

Zuwachs hat die Familie von Solid State Disks im 19-Zoll-Format von Texas Memory Systems (www.superssd.com) bekommen. Der RamSan-440 getaufte Neuzugang erreicht mit 256 oder 512 GByte DDR2-SDRAM die zwei- respektive vierfache Kapazität im Vergleich zu seinem Vorgänger. Die I/O-Leistung stieg mit 600 000 Zugriffen pro Sekunde um 50 % bei einem Durchsatz von 4500 MByte/s und einer Latenz von unter 15 µs. Leider stieg auch der Stromverbrauch von 350 auf 650 Watt.

Als Backup-Speicher verwendet der RamSan-440 nun 5 SSDs auf NAND-Flash-Basis (RAID 3). Redundante Pufferbatterien geben dem Gerät bei einem Stromausfall 25 Minuten Zeit, die Daten dorthin zu kopieren. Bei wiederhergestellter Stromzufuhr benötigt das 512-GByte-Modell knapp sechs Minuten, um den gesamten Speicherinhalt zurückzuschreiben.

Verfügbar sein soll eine FC-Variante mit zwei bis acht 4-GBit/s-Ports sowie eine 4x-Infiniband-Version mit einem bis vier 10-GBit/s-Anschlüssen.

IEEE 1394-2008: Firewire mit 3,2 GBit/s noch in diesem Jahr

Für Oktober plant die IEEE die dritte Version des 1394/Firewire-Standards. 1394-2008 sieht Verbindungen mit 1,6 (S1600) respektive 3,2 GBit/s (S3200) vor. Dabei soll die Kompatibilität mit den bisherigen Schnittstellen IEEE 1394 (400 MBit/s) und 1394b (800 MBit/s) jedoch gewahrt bleiben.

Dieser Schritt scheint eine Reaktion darauf zu sein, dass die Konkurrenz aus dem USB-Lager mit USB 3.0 eine 5 GBit/s schnelle Version aus der Taufe heben will. Deren Spezifikation soll aber erst im nächsten Jahr erscheinen, sodass Firewire zumindest einen zeitlichen Vorsprung hat. Allerdings soll der „Superspeed USB“ genannte Universal Serial Bus 3.0 mit Lichtwellenleitern arbeiten. Inwieweit sich das im Desktop-Bereich bewährt und welchen Durchsatz er tatsächlich erreicht, bleibt abzuwarten. Schon USB 2.0 überträgt netto nur gut die Hälfte der theoretischen 480 MBit/s.

Neue Signalprozessoren von TI

Stromspar-Quartett

Axel Urbanski

Texas Instruments erweitert die vier DSP-Produktlinien C67, C64+, C55 und Omap um Modelle mit geringem Energiebedarf.

Keine völlig neu entwickelten DSPs, sondern Strom sparende Versionen seiner bekannten Signalprozessor-Linien bringt Texas Instruments (www.ti.com) auf den Markt.

Bei der neuen Familie Omap-L1x handelt es sich nicht um einen DSP (Digital Signal Processor) im klassischen Sinn, sondern um einen asymmetrischen Multi-Core-Prozessor mit unterschiedlichen Prozessorkernen auf einem Chip. Als Grundlage dient eine 300 MHz schnelle ARM-9-CPU. Je nach Modell kommt ein Audio-Koprozessor oder ein DSP-Kern als Ergänzung hinzu. Zur Wahl stehen ein 24/32-Bit-Floating-Point-DSP aus der C674x-Familie und ein 16/32-Bit-Fixed-Point-DSP (C64x+).

Als Schnittstellen bietet der Omap-L1x einen DMA-Port zum Host, UARTs, ein Serial Peripheral Interface (SPI), I^2C sowie Anschlüsse für MMC/SD-Karten, USB 2.0 sowie SATA. Laut Hersteller bewegt sich der Stromverbrauch zwischen 6 Milliwatt im Schlafmodus, 11 mW im Standby und 435 mW im Betrieb. Bislang kommen die Chips vor allem in mobilen Geräten wie Handys oder MP3-Playern zum Einsatz.

Die neuen 24/32-Bit-Fließkomma-DSPs der TMS320 C674x-Familie glänzen durch einen ähnlich niedrigen Energieverbrauch von 6, 11 beziehungsweise 420 Milliwatt. Bei einem Takt von 300 MHz erreichen sie eine maximale Rechenleistung von 2400 MMACs (Million Multiply Accumulate Cycles per Second). Ihre Ausstattung ähnelt der des Omap-L1x. Genügt Festkomma-Arithmetik, kann ein 16/32-Bit-Prozessor aus der TMS320C640x-Familie zum Einsatz kommen. Er bietet dieselbe Leistung wie sein Vetter und kommt dabei sogar mit etwas weniger Strom aus (415 mW). Beide sind pinkompatibel zum Omap-L1x.

Besonders sparsam gibt sich der mit 16 Bit (Fixed Point) rechnende TMS320C550x: Im Betrieb saugt der Signalprozessor bei einem Takt zwischen 60 und 100 MHz 18 bis 46 mW aus dem Akku, im Standby-Modus 0,34 mW und im Tiefschlaf lediglich 6,8 µW.

Die in der Signalverarbeitung häufig benötigte Fast-Fourier-Transformation (FFT) delegiert der DSP an einen integrierten 24-Bit-Koprozessor, der bis zu zehn Transformationen mit reellen oder komplexen Zahlen ausführen kann. Kontakt zur Außenwelt kann der DSP über UARTs, USB 2.0, SDIO, SPI oder das Inter-IC Sound Interface (I^2S) aufnehmen. (mr)

iX-Link ix0809030

Isolierende Treiberbausteine für RS232 und RS485

Während bei Notebooks und PCs die serielle Schnittstelle fast ausgestorben ist, bleibt sie in der rauen Industrieumgebung unverzichtbar. Dort gelten jedoch härtere Anforderungen, etwa im Hinblick auf die galvanische Trennung von Systemen. Analog Devices (www.analog.com) hat mit dem ADM3251E einen geeigneten Treiber für RS232-Verbindungen vorgestellt, der eine Isolationsspannung von 2500 V aufweist. Im Gegensatz zu anderen verwendet er zur Potenzialtrennung keine Optokoppler, sondern On-Chip-Transformatoren, wodurch sich ein höheres Übertragungstempo erreichen lässt: Der ADM3251E sendet und empfängt mit bis zu 460 kBit/s. Für RS485-Busse eignet sich der Vollduplex-fähige ADM2484E, der maximal 500 kBit/s erreicht.

Axel Urbanski



Multitouch-Controller von Cypress

Cypress (www.cypress.com) erweitert sein Angebot an Touchscreen-Controllern für mobile Geräte um mehrere Multitouch-Controller. Unter der Flagge „True Touch“ segeln nunmehr drei unterschiedliche Techniken: das klassische Einfinger- oder Single-Point-Verfahren sowie Multitouch-Techniken für zwei und zehn Finger, die auch Gesten verstehen.

Der 10-Finger-Controller CY8CTMA120 bedient Displays bis zu einer Diagonalen von 8,5 Zoll. Sein integrierter M8C-Prozessor mit Harvard-Architektur verfügt über 1 KByte Datenspeicher (RAM) sowie 16 KByte Flash-Speicher für Programme. Die Entwicklungsumgebung PSoC Designer gibt es kostenlos dazu; eine Bibliothek mit Routinen zur Gestenerkennung gehört zum Lieferumfang. Zweifinger-Bedienung lässt sich mit dem CY8CTMG120 realisieren, der sonst seinem großen Bruder entspricht.

Mit einer zusätzlichen SPI-Schnittstelle und nur 1,9 mA Stromaufnahme – 9,5 mW bei einer Betriebsspannung von 5 V – empfiehlt sich der CY8CTMG100. Sein Vetter CY8CTMG110 begnügt sich mit einem I^2C-Bus-Interface, saugt jedoch 4 mA (20 mW) aus der Batterie. Beide sind für Displays mit Diagonalen bis 4 Zoll gedacht und mit je 512 Byte RAM sowie 8 KByte Flash-Speicher ausgestattet. Die Serienproduktion soll im September beginnen.

Axel Urbanski



System on a Chip mit Pentium-M-Prozessor

Intel (www.intel.com) hat mit dem EP80579 ein vielseitiges System on a Chip (SoC) angekündigt. Es enthält einen Pentium-M-Kern (Banias) mit 256 KByte L2-Cache. Ab 2009 soll stattdessen Intels Stromspar-Prozessor Atom zum Einsatz kommen. Ein optionaler Krypto-Koprozessor nimmt der CPU rechenintensive Aufgaben wie Verschlüsselung ab.

Der Integrated Memory Controller Hub verbindet CPU, 64 Bit breites DDR2-SDRAM und Peripherie miteinander. Seine acht PCI-Express-Lanes lassen sich wahlweise in einer 1×8-, 2×4- oder 2×1-Konfiguration betreiben. Weitere Schnittstellen bietet der Integrated I/O Hub: ein Serial Peripheral Interface (SPI), das auch zum Booten dient, einen Low Pin Count Bus (LPC 1.1), je zwei SATA-II- und USB-2.0-Schnittstellen, UARTs und SMBus/I^2C-Interfaces sowie 36 zusätzliche GPIO-Leitungen (General Purpose I/O).

Im „I/O Complex“ finden sich drei Gigabit-Ethernet-Schnittstellen (MACs), ein WAN-Interface (T1/E1), eine synchrone serielle Schnittstelle (SSP) sowie ein 16 Bit breiter Erweiterungsbus. Ein CAN-Bus-Anschluss (Controller Area Network) erlaubt den Einsatz im industriellen oder Automobil-Umfeld. Intel bietet die Chips für Taktfrequenzen von 600 MHz, 1,066 und 1,2 GHz an. Ihre Leistungsaufnahme variiert zwischen 11 und 19 W; die Krypto-Engine benötigt 2 Watt zusätzlich. *Axel Urbanski*

iX-Link ix0809030

Ausgaben für Kundenbindung steigen

Laut jährlicher Statistik der Gartner Group legten die Umsätze im weltweiten CRM-Markt 2007 um satte 23,1 % auf insgesamt 8,1 Mrd. Dollar zu. Insbesondere die Schwellenländer, die schnelle Adaption von Software as a Service (SaaS) sowie die steigenden Investitionen in Kundenbindungsmaßnahmen bescherten CRM-Anbietern das anhaltende Wachstum. Allerdings machen sowohl SaaS und die aufstrebenden Regionen gerade einmal 15 % des Marktvolumens aus. Nummer 1 unter den Herstellern ist weiterhin SAP. Auch wenn der Marktanteil ein wenig schrumpfte, konnte man Oracle weit hinter sich lassen. Unverändert an dritter Stelle liegt Salesforce.com. Der Pionier bei den Mietlösungen kann jedoch mit einem erheblich höherem Wachstum als SAP und Oracle aufwarten. Nur Microsoft legte stärker zu.

CRM-Anbieter weltweit

Unternehmen	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil	Wachstum
SAP	2,0501	25,4	1,682	25,6	22,0
Oracle	1,320	16,3	1,017	15,5	29,8
Salesforce.com	0,677	8,4	0,452	6,9	49,8
Amdocs	0,421	5,2	0,366	5,6	15,1
Microsoft	0,332	4,1	0,176	2,7	88,6
andere	3,289	40,6	2,882	43,7	14,1
gesamt	8,089	100,0	6,574	100,0	23,1

Marktanteile und Wachstum in Prozent, Umsatz in Mrd. Dollar
Quelle: Gartner 7/2008

Infor baut PLM-Lösung aus

Ein neues Release seiner Product-Lifecycle-Anwendung für Prozessfertiger und Händler mit Eigenmarken kündigte Infor an. Neu in Optiva ist der Advanced Formula Editor, der Unternehmen helfen soll, Rezepturen und Varianten zu modellieren, auf dieser Basis Zusammensetzungen festzulegen und mögliche Risiken zu erkennen. Überarbeitet hat man das Analysemodul für die Simulation des Produktdesigns in der Fertigung. Damit lassen sich kritische Bereiche früher entdecken, kostspielige Änderungen in der Herstellungs- und Logistikkette sollen so gar nicht erst anfallen. Eingebunden in Optiva ist Atrions Software zum Management der Produkt-Compliance. Die Anwendung bereitet die Produktanalyse auf gesetzliche Anforderungen vor. Sie automatisiert etwa die Erstellung von weltweit gültigen, mehrsprachigen Dokumenten.

IBM übernimmt Ilog

Die Spekulationen sind beendet: IBM kauft das französische Softwarehaus Ilog für rund 215 Mio. Euro. Den Analysten von PAC zufolge weckte insbesondere dessen Business-Rules-Managementsystem die Begierde, denn es passe genau in IBMs SOA-Strategie. Die weiteren Ilog-Produkte – etwa Supply-Chain- sowie Visualisierungslösungen – gelten nur als schmückendes Beiwerk. Laut IDC profitiert IBM zudem vom starken OEM-Geschäft der Franzosen, über 500 Softwarehäuser haben Ilog-Routinen in ihre Produkte eingebaut. Dass die Kunden indes von der Übernahme begeistert sind, darf bezweifelt werden. SAP beispielsweise setzt Ilog-Algorithmen in seinem SCM/APO-Produkten ein. Allerdings konkurriert SAP selbst nach der Akquisition von Yasu Technologies beim Regelmanagement mit Ilog. Mit der Übernahme nimmt die ohnehin hohe Konzentration auf dem Plattform-Markt weiterhin zu. Analysten vermuten, dass der Aufkauf kleinerer Spezialisten wie Fair Isaac oder Pegasystems nur eine Frage der Zeit ist.

SAP kassiert mehr für Wartung

Nun ist es offiziell: Ab Januar 2009 wird SAPs Serviceprogramm Enterprise Support für alle Kunden verbindlich. Bis Ende 2008 dürfen sie die erweiterten Dienstleistungen kostenfrei nutzen. Danach erhöhen sich die Wartungsgebühren über vier Jahre stufenweise von heute 17 % auf 22 % (im kommenden Jahr auf 18,3 %). SAP begründet die Preissteigerung mit einem größeren Support-Umfang. Unklar ist, ob der Enterprise Support für jeden Anwender wirklich einen echten Mehrwert bietet oder für Mittelständler überdimensioniert ist, wie die DSAG (Deutschsprachige SAP-Anwendergruppe) befürchtet.

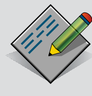
Mehr Optionen für Corebiz

Die LIS AG hat ihre Open-Source-Unternehmenssoftware Corebiz in der Version 3.1 veröffentlicht. Das Produkt für mittelständische Unternehmen und öffentliche Einrichtungen bekam zusätzliche Managementoptionen spendiert. Ubuntu 8.04 LTS (Long Term Support) fungiert jetzt als Betriebssystem. Herzstück der Software ist der Linux-Server mit OpenLDAP-basiertem Verzeichnisdienst. Alle Module werden über eine zentrale Anwendung konfiguriert und gesteuert. Die Integration des Common Unix Printing Systems (CUPS) in die Managementkonsole soll die Installation von Druckertreibern und Netzwerkdruckern vereinfachen. Hier lassen sich auch unterschiedliche Ansichten für verschiedene Benutzergruppen einstellen. Zudem unterstützt der Corebiz-Client Roaming-Profile.

BAM und BI kooperieren

Der Activity Monitor von iWay führt Information Builders Business-Intelligence-Plattform Webfocus und die Überwachung von Geschäftsprozessen (Business Activity Monitoring, BAM) zusammen. iWay ist eine Tochtergesellschaft von Information Builders. Das so entstandene Kontrollinstrument misst Unternehmenskennzahlen in Geschäftsprozessen und bereitet die Daten in einem Dashboard grafisch auf. Beispielsweise soll es bei überschrittenen Grenzwerten Alarm auslösen sowie Kapazitätsengpässe und andere Störungen im Betriebsablauf erkennen.

KURZ NOTIERT



Aufgabe: SAP stellt Tomorrow Now bis Ende Oktober ein. Das Tochterunternehmen, das die Walldorfer im Februar 2005 gekauft hatten, leistet Support für Oracle- und andere Anwendungen. Hier liegt die Ursache des Rechtsstreits mit Oracle über den Diebstahl von Firmengeheimnissen. Die rund 225 Tomorrow-Now-Kunden will SAP beim Wechsel auf einen Oracle-Wartungsvertrag oder andere Support-Optionen unterstützen.

Ausbau: Auf der DMS stellt Docuware eine erweiterte Version seines Webclients vor. Markierungen und Anmerkungen kann der Benutzer jetzt direkt in einem Dokument vornehmen. Auch die aus dem traditionellen Windows-Client gewohnten Zeichenwerkzeuge lassen sich jetzt über das Internet bedienen.

ERP-Game: Das neue Lernspiel von Poolix soll den Anwendern spielerisch SAP-Geschäftsprozesse vermitteln. Die Software beschäftigt sich mit dem Aufbau der Systeme und gibt einen Überblick über die Module Vertrieb, Materialwirtschaft, Produktion sowie Finanzen und Controlling. Ein bis drei Teilnehmer spielen ein konkretes Szenario (Minitruck GmbH) nach.

KURZ NOTIERT

Gewachsen: Die BTC Business Technology Consulting AG schloss das Geschäftsjahr 2007 mit einem Umsatz von 112,3 Mio. € ab. Damit verzeichnet das Oldenburger IT-Servicehaus im dritten Jahr in Folge eine dreißigprozentige Steigerung des Umsatzes. Ein Teil des Zuwachses geht auf die Übernahme mehrerer Firmen zurück.

Aufkauf: Open Text, Anbieter von Enterprise-Content-Management-Software, hat der Corbis Corporation die Emmotion LLC abgekauft. Das Unternehmen wird in die Artesia Digital Media Group von Open Text eingegliedert und erweitert deren Angebot für das Digital-Media-Management.

Lehrling: Oracle setzt die Einkaufstour fort. Jüngstes „Opfer“ wurde der Lern- und Trainingssoftwareanbieter Global Knowledge Software. Mit der Übernahme soll das Geschäft für Trainingslösungen des Softwarekonzerns ausgebaut werden.

Einstieg: Die japanische NTT Data Corporation wird neuer Mehrheitsgesellschafter des Münchener Beratungsunternehmens Cirquent. Der bisherige Eigner BMW bleibt als Gesellschafter an dem IT-Serviceunternehmen beteiligt. Cirquent war Anfang 2008 aus der ehemaligen Softlab-Gruppe hervorgegangen.

Besser als erwartet: Ein solides Schlussquartal im Geschäftsjahr 2008 bescherte Cisco eine erstaunliche Jahresbilanz. Der Netzwerkausrüster steigerte die Einnahmen um 13,2 % auf insgesamt knapp 40 Mrd. $. Der Reingewinn konnte um rund 10 % auf 8,1 Mrd. $ gesteigert werden.

Microsofts Bilanz 2008

Nach oben offen

Achim Born

Microsoft knackte im Geschäftsjahr 2008 erstmals die 60-Mrd.-$-Umsatzmarke. Die Einnahmen mit traditionellen Softwareprodukten prägen weiterhin das Geschäft.

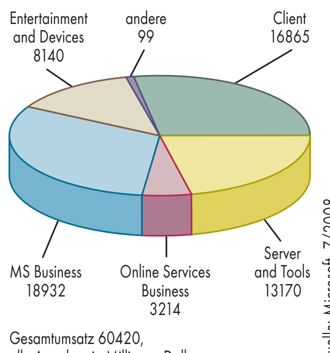
Microsoft hat enttäuscht, wieder einmal. Ein Gewinnsprung im Schlussquartal des am 30. Juni beendeten Geschäftsjahres von 42 % auf 4,3 Mrd. $ war den Börsianern einfach nicht genug. Selbst die Entwicklung der Einnahmen (15,84 Mrd. $, +18 %), die über den Erwartungen lag, konnte die Stimmung der Anleger nicht aufhellen. Hinzu kommt der Ausblick auf das neue Geschäftsjahr, der Enttäuschungen bereithält. Der nunmehr prognostizierte Umsatz zwischen 67,3 Mrd. und 68,1 Mrd. $ wie auch der Gewinn pro Aktie (2,12 bis 2,18 $) liegen unter den Erwartungen. Als Grund für die revidierten Aussichten werden von den Microsoft-Oberen zusätzliche Investitionen in das Internetgeschäft angeführt. Ebenso verweisen Analysten auf den enttäuschenden Verlauf des Internetanzeigengeschäfts bei Microsoft, auf das die Investoren angesichts des Gerangels um Yahoo ein besonderes Augenmerk haben.

Lässt man die Wetten um künftige Erlöse jedoch außen vor, lief die gut geölte Maschine wieder wie gewohnt. Der Umsatz stieg um 18 % auf 60,42 Mrd. $. Der Nettogewinn legte um 26 % auf 17,681 Mrd. $ zu. Der häufig kolportierte Einbruch aufgrund der schwächelnden US-Konjunktur ist folglich nicht zu sehen. Im Gegenteil, denn in den klassischen Geschäftssparten konnten die Redmonder noch einmal kräftig zulegen. So stieg der Umsatz der Windows-Sparte (Client-Segment) im Schlussquartal um fast 15 % auf 4,37 Mrd. $. Die Server&Tool-Sparte schnellte um 22 % auf 3,74 Mrd. $ hoch. Und selbst die Einnahmen im Business-Bereich (Office und Unternehmenssoftware), die unter den Erwartungen blieben, legten um 14 % auf 5,26 Mrd. $ zu. Die Umsätze mit Online Services (838 Mio. $, +24 %) fallen im Vergleich zu den anderen Sparten noch gering aus.

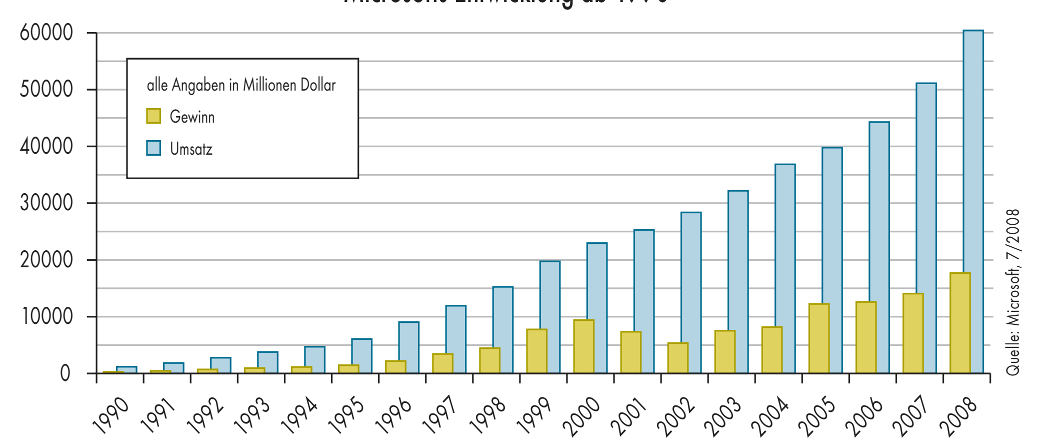
Das Unterhaltungssegment (vornehmlich XBox) wuchs immerhin um ein Drittel auf 1,575 Mrd. $. Im Bereich Entertainment wies Microsoft im Schlussquartal wieder einen, wenn auch überschaubaren Verlust (188 Mio. $) aus. In der Jahresgesamtsicht blieb unter dem Strich immerhin ein Plus von 426 Mio. $ bei rund 8 Mrd. $ Einnahmen übrig. Noch im Vorjahr verunstaltete hier ein sattes Minus von 2 Mrd. $ die Bilanz. Verluste fuhr ebenso der Hoffnungsträger Online ein. Sie betrugen im Schlussquartal 488 Mio. $ und im Geschäftsjahr 1,23 Mrd. $ (Umsatz: 3,2 Mrd. $).

Als Goldgrube erwies sich wieder einmal das Windows-Geschäft. Die Sparte wies bei einem Gesamtumsatz von 16,865 Mrd. $ einen Gewinn von 13 Mrd. $ aus. Das Schlussquartal steuerte 3,2 Mrd. $ bei. Das Business-Segment stellte weiterhin den zweiten Gewinnbringer dar. Hier blieben am Ende des Jahres bei einem Umsatz von knapp 19 Mrd. $ unter dem Strich 12,36 Mrd. $ (Schlussquartal: 3,34 Mrd. $) übrig. Dagegen wirkte sich der Gewinn mit Server&Tools in Höhe von 4,6 Mrd. $ bei 13,2 Mrd. $ Einnahmen vergleichsweise gering aus. (WM)

Segmentumsatz im Jahr 2008



Microsofts Entwicklung ab 1990



SAP gelingt gutes Quartalsergebnis

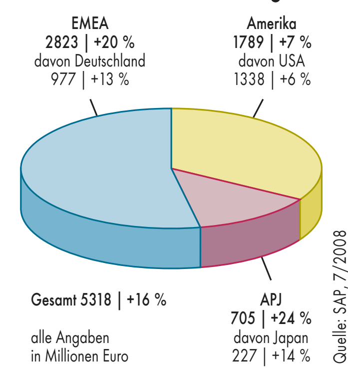
Viel verdient

Achim Born

Mit der starken Steigerung der Einnahmen konnte SAP sehr zufrieden sein, mit der mäßigen Erhöhung der Gewinne wohl eher nicht.

Der SAP-Boss Henning Kagermann freute sich: „Wir haben hervorragende Ergebnisse im 2. Quartal erzielt.“ In Zahlen heißt das: Die weltweiten Einnahmen aus dem Softwaregeschäft stiegen um 21 % auf 2,06 Mrd. €. Nimmt man einmalige Abschreibungen auf abgegrenzte Support-Erlöse aus der Akquisition von Business Objects heraus, betrug das Plus sogar 24 %. Mit Blick auf die Ergebnisse des Erzrivalen Oracle rechnete sich SAP zudem einmal in Dollar „schön“. Danach wären beispielsweise die Software- und softwarebezogenen Serviceerlöse um satte 44 % gegenüber der Vorjahresperiode angestiegen.

Gesamtumsatz nach Region



Quelle: SAP, 7/2008

Im realen Wirtschaftsleben bleibt dem Walldorfer Softwarehaus jedoch nichts anderes übrig, als den starken Euro als Wachstumsdämpfer zu akzeptieren. Ein Plus von 18 % auf 2,86 Mrd. € kann sich aber auch ohne Bereinigung sehen lassen. Die Softwarelizenzerlöse erhöhten sich um 25 % gegenüber der Vorjahresperiode auf 898 Mio. €. Das Support-Geschäft steuerte 1,099 Mrd. € (16 %) zu. Beratung und Schulung trugen 768 Mio. € (12 %) bei. Im ersten Finanzhalbjahr erzielte SAP einen Gesamtumsatz von 5,32 Mrd. € (+16 %) beziehungsweise von 5,42 Mrd. € (+20 %), wenn die Abschreibungen herausgerechnet werden. Die Software- und Serviceerlöse stiegen um 18 % gegenüber der Vorjahresperiode auf 3,80 Mrd. €. Die Lizenzerlöse erhöhten sich um 19 % auf 1,52 Mrd. €. Beratung und Schulung steuerten knapp 1,5 Mrd. € (+12 %) bei.

Im Unterschied zum Umsatz erfüllte SAP beim Gewinn die Erwartungen nicht. Der Konzernüberschuss schrumpfte im ersten Halbjahr um 14 % auf 650 Mio. €. Beim Betriebsergebnis (952 Mio. €) betrug der Rückgang 6 %.

(WM)

Reif für die Insel

Der ITK-Markt Großbritanniens, mit 152 Mrd. € Umsatzspitzenreiter in Europa, sollte das Interesse deutscher Anbieter wecken. Zumindest ist die regionale Wirtschaftsförderungsgesellschaft Advantage West Midlands davon überzeugt. Sie entwickelte die einmalige Förderinitiative „Bridge-to-Growth“ (www.bridgetogrowth.de), um hiesigen Firmen den Sprung über den Kanal zu erleichtern. Interessenten müssen lediglich zwei Kriterien erfüllen: das Unternehmen sollte nicht mehr als 750 Beschäftigte haben und die Gründung einer Tochtergesellschaft in Großbritannien planen. Zur Förderung gehören ein kostenloses Expertenseminar und ein Start-up-Paket mit Leistungen wie Büroräumen während der Markteintrittsphase sowie Gründung der Limited.

IT-Servicemarkt bleibt auf Wachstumskurs

Ungeachtet der schwachen Konjunktur werden die weltweiten Ausgaben für IT-Services 2008 um 9,5 % zulegen und damit ein Gesamtvolumen von 819 Mrd. $ erreichen. Zu diesem Schluss kommt die US-Beratung Gartner auf Basis der Entwicklung in den ersten sechs Monaten des laufenden Jahres. Bis 2012 erwarten die Analysten ein dauerhaftes Wachstum, die Billion-Dollar-Hürde ist dann überschritten. Die erfreuliche Entwicklung des Gesamtmarktes ist nach Auskunft von Gartner nicht allein den vertrieblichen Erfolgen geschuldet, sondern beruht zum Teil auch auf der anhaltenden Dollarschwäche. Da viele Verträge auf anderen Währungen wie dem Euro beruhen, führt die Umrechnung auf Dollar zwangsweise zu einem rein rechnerischen Plus.

IT-Services weltweit

Segment	2007	2008	2009
Consulting	64,656	71,002	75,500
Entwicklung&Integration	232,452	256,045	272,356
IT Management	201,222	220,606	234,433
Process Management	110,694	121,353	132,250
Hardware-Support	89,654	94,691	97,269
Software-Support	49,346	55,409	60,636
Gesamtmarkt	748,025	819,106	872,454

alle Angaben in Milliarden Dollar

Quelle: Gartner 7/2008

Spezialisten-Ranking: Business Intelligence

Das Marktforschungsunternehmen Lünendonk schätzt das deutsche Marktvolumen von BI-Software inklusive Services für 2007 auf etwa 710 Mio. €. Rund 45 % des Marktvolumens entfallen demnach auf die 15 führenden BI-Unternehmen, mit einem gemeinsamen Inlandsumsatz in Höhe von 318,9 Mio. € und mit einem durchschnittlichen Wachstum gegenüber dem Vorjahr von 24,8 %. Informatica (+ 70,9 %), Qliktech Deutschland (+ 64,9 %), Cubeware (+ 46,6 %), Idl (+ 38,5 %) sowie CSS (+ 28,6 %) konnten sogar überdurchschnittlich zulegen. Allerdings gelang es der SAS Deutschland GmbH, trotz eines unterdurchschnittlichen Plus von 6,7 % die Marktführerschaft in Deutschland zu behaupten. Mit einem geschätzten Umsatz von 96 Mio. € erzielte das Unternehmen einen fast doppelt so hohen Umsatz wie Cognos, das mit geschätzten 50 Mio. € Platz 2 der Lünendonk-Liste belegt.

Business Intelligence in Deutschland

Rang	Unternehmen	Umsatz 2007	Umsatz 2006	Mitarbeiter 2007	Mitarbeiter 2006
1	SAS Deutschland	96,0	90,0	435	400
2	Cognos	50,0	42,0	170	140
3	Business Objects	40,2	40,0	90	106
4	Teradata	28,5	25,7	195	162
5	Microstrategy	19,4	18,5	57	45
6	SPSS	13,7	12,9	65	63
7	Arcplan	9,9	9,5	52	50
8	Informatica	9,4	5,5	45	30
9	Qliktech	9,1	5,5	65	40
10	Cubeware	8,5	5,8	83	59
11	Corporate Planning	8,0	6,6	92	83
12	CSS	7,2	5,6	61	59
13	Idl	7,2	5,2	60	54
14	Winterheller	6,0	5,0	39	44
15	Actuate	5,8	4,5	19	15

Umsatz Zahlen in Millionen Euro

Quelle: Lünendonk GmbH, 7/2008



Deutschsprachige Onlinenetz-Szene

Schwarmgefühl

Ramon Wartala

Ob geschäftlich oder privat: Soziale Netze bieten – angemeldeten – Nutzern ein warmes Nest, in dem sie sich mit Gleichgesinnten austauschen können. Und Werbeflächen sollen für Umsatz sorgen. In deutschsprachigen Landen gibt es für fast jeden zwei bis drei solcher Gemeinschaften.

Mitmachnetze bieten sich für fast alle nur denkbaren Themen an. Büchernarren wie Fußballfans kommen ebenso auf ihre Kosten wie Schüler, Studenten und junge Eltern. Mitmachen in einem der vielen Onlinenetze ist kinderleicht, die Software hat sich nicht zuletzt dank des Web 2.0 zu ausgereiften Produkten entwickeln können. Alles wäre gut, wenn es nicht Identitätsdiebe und Betrüger gäbe – siehe den folgenden Artikel. Ein weiterer Text zeigt, wie Dritte Anwendungen für die sozialen Netze schreiben können.

Mitmachen in mehrerlei Bedeutung konnte man im Internet schon lange. Es kommt darauf an, was man darunter versteht. Ray Tomlinson von Bolt, Beranek und Newman (BBN, die Firma, die den Anfang des Internet als Arpanet entwickelte) hat Ende 1971 die anscheinend erste E-Mail verschickt, in der er vor allem erklärte, warum er das @-Zeichen als Trenner zwischen Benutzer und Host benutzt. Zwar konnten in den Siebzigerjahren kaum Menschen das Internet (das noch kein WWW beinhaltete) nutzen, aber die wenigen, die Zugang zu vernetzten Rechnern hatten, konnten kommunizieren – allerdings asynchron.

Chat bot schon das alte BTX, und was heute Foren sind, hieß seit Ende der Siebzigerjahre Usenet. Wer in den Achtzigerjahren online ging, fand im Usenet jede Menge Newsgruppen vor, in denen Nutzer weltweit die Computerei in allen Spielarten diskutierten, aber sich darüber hinaus über Literatur, Rezepte und dergleichen mehr austauschten. Als 1985 der Whole Earth ’Lectronic Link (WELL) seine Pforten öffnete, begann die Zeit der virtuellen Gemeinschaften, die einer der ersten Nutzer, Howard Rheingold, in den Neunzigerjahren analysierte [g]. Und die WELL-Nutzer organisierten gelegentlich Treffen im RL (real life).

Dank des World Wide Web sehen Foren heute anders aus als „damals“, und dank Breitbandverbindungen gestaltet sich die Kommunikation gelegentlich fast in Echtzeit. Nicht zu vergessen: Das Web 2.0 bietet Entwicklern wie Anwendern unvergleichlich viel mehr als Usenet oder das Web 1.0.

Pflege geschäftlicher Kontakte

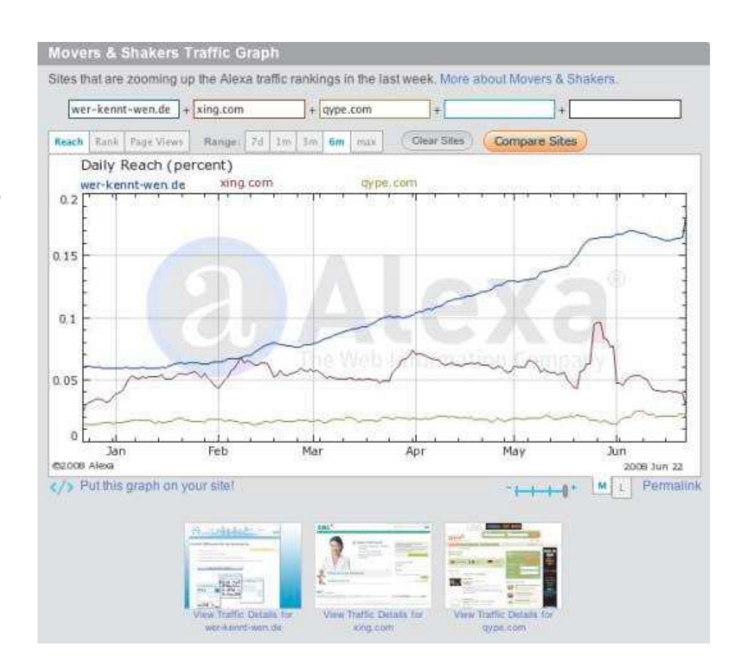
Unter dem Namen OpenBC im Jahre 2003 gegründet und seit Mitte 2007 bekannt als Xing, hat sich diese Plattform für geschäftliche Kontakte längst etabliert. Laut FAZ.net vom 22. Juli dieses Jahres (siehe *iX*-Link) hat Xing derzeit gut sechs Millionen Mitglieder (davon 470 000 monatlich 5,95 € zahlende). Im Unterschied zu einem Forum bietet ein Netz-im-Netz wie Xing die Option, sich selbst vorzustellen, seine berufliche Erfahrung und seine Interessen darzustellen. Der Gemeinschaftsaspekt entsteht durch die bidirektional gespeicherten Kontakte zu anderen Netzmitgliedern, Diskussionsrunden können öffentlich wie gruppenintern gehalten sein. Eine „Community“ muss daraus allerdings nicht entstehen, denn vor allem geht es um Kontaktpflege.

Jenseits der sogenannten Big Player – neben xing.com vor allem facebook.de und myspace.com – hat sich in Deutschland eine beachtliche Zahl sozialer Netze etabliert, die nach jüngsten Zahlen der Arbeitsgemeinschaft Online-Forschung (AGOF, siehe [d]) mit Reichweiten über der Millionengrenze glänzen können. Neben alten Bekannten wie studivz.de, schülervz.de und stayfriends.de überspringen Dienste die Millionen-Benutzer-Grenze, die bislang weniger im Licht der Öffentlichkeit standen. Dazu zählen Chat-Portale wie knuddels.de oder lokalisten.de. Nahe an der Millionengrenze schrappen piczo.com, das Freunde-Portal kwick.de und jux.de vorbei. Abseits des Mainstreams existieren ebenfalls eine Reihe gut besuchter Mitmach-Webseiten, die die unterschiedlichsten Zielgruppen bedienen. Da gibt es Netze für spezielle Berufs- und Altersgruppen, Hobbys und Haustiere. Allen gemein ist das Ziel, dass sich viele Mitglieder bei ihnen anmelden und vor allen Dingen lange aktiv

bleiben. Denn nur so bleibt die Plattform für neue Nutzer und die werbetreibende Industrie attraktiv.

Viele dieser Netze scheuen bewusst den Aufwand und die Kosten einer AGOF-Messung, deshalb lässt sich auf den ersten Blick nur schwer erkennen, welches wirklich über eine aktive Nutzerschaft verfügt. Erste Anhaltspunkte über die Aktivität einer Community geben Dienste wie Alexa oder Google Trends [e] – siehe Abbildung 1.

Thematisch begrenzte Netze können wesentlich eher den Charakter einer Gemeinschaft haben, weil sie sich um Familie, Autos, Bücher, Musik oder beliebige andere konkrete „Dinge“ drehen. Das Interesse an ihnen bestimmt das Geschehen im Onlinenetz. Ihre Zahl geht allmählich an die 200 (siehe [b, c, f]). Von Konsolidierung kann momentan noch keine Rede sein.



Vergleich der Alexa-Rankings für wer-kennt-wen.de, xing.com und qype.com – am besten schneidet Xing ab (Abb. 1).

Fazit

Der gemeine deutsche beziehungsweise deutschsprachige Internetnutzer kann auf eine Fülle sozialer Netze zugreifen. Allerorts locken kostenlose Mitgliedschaften den kommunikativen Surfer. Kostenlos aber nur insofern, als Nutzer keinen Mitgliedsbeitrag entrichten müssen. Das neu registrierte Mitglied soll gleich viele eigene Inhalte auf die Plattform stellen. Diese haben die Betreiber schließlich nicht zum Spaß, sondern für viel Geld programmiert, und sie läuft auf Servern, die ihrerseits bezahlt werden wollen. Zahlungskräftige Werbekunden locken die Plattform-Verantwortlichen direkt, über Affiliate-Netze oder Onlinevermarkter auf die



Deutsche Onlinenetz-Szene

Allgemein	
Bloomstreet	bloomstreet.net
Facebook	www.facebook.de
Jux	www.jux.de
Knuddels	www.knuddels.de
Kwick	www.kwick.de
Lokalisten	lokalisten.de
Myspace	myspace.de
Piczo	www.piczo.com
Stayfriends	www.stayfriends.de
Uboot	www.uboot.com
Unddu	unddu.de
Familie	
1-2-3family	www.1-2-3family.de
Babyvoten	babyvoten.de
Family Lounge	www.familylounge.de
Ich bin Papa	ichbinpapa.de
Mamacommunity	www.mamacommunity.de
Mamily	mamily.de
Mamiweb	mamiweb.de
Mummynetwork	mummynetwork.com
Netmoms	www.netmoms.de
Geschäftlich	
Come United	www.comeunited.com
Grafiker	www.grafiker.de
Mediap	www.mediap.de
Mycorners	mycorners.com
Theweps	www.theweps.com/de/doing_business.html
Wer kennt wen	www.wer-kennt-wen.de
Xing	www.xing.com
Haustiere	
Deine Tierwelt	www.deine-tierwelt.de
Dognetwork	dognetwork.de/home.php
Hallo Hund	www.hallohund.de
Mycat	www.mycat.de
Mywuff	www.mywuff.com/index.php
Stadthunde	stadthunde.com
Tiercommunity	www.tiercommunity.com
Tierfc	www.tierfc.de
Tierfreunde	www.tierfreunde.de
Lesen	
Alexandria	www.buch.de/shop/home/alexandria/
Lesenswert	lesenswert.net
Lovely Books	www.lovelybooks.de
Reisen	
Digitalreise	www.digitalreise.de
Globalzoo	www.globalzoo.de
Tag your place	tagyourplace.com
Tripflip	www.tripflip.de
Tripsbytips	www.tripsbytips.de
Vagabund	vagabund.biz
Schüler	
Abitreff	www.abitreff.de
Schüler.CC	www.schueler.cc
Schülerprofile	www.schuelerprofile.de
Schülerregister	schuelerrg.de
SchülerVZ	www.schuelervz.net
Spickmich	www.spickmich.de
Sport	
Dein Fussball	deinfussball.de
Die Fans	www.die-fans.de
Jogmap	www.jogmap.de
KletterVZ	klettervz.de
Kletterzentrale	kletterzentrale.de
Klubba	klubba.de
Mein Fußballclub	meinfussballclub.de
Mein Sportplatz	meinsportplatz.de
Mein Verein	www.meinverein.de/home
Mylaola	www.mylaola.de
Netzathleten	www.netzathleten.de
Soccerspin	soccerspin.de
Sport-ID	sport-id.de
Sportiversum	www.sportiversum.de
Sportme	sportme.de
Sportsfreunde	www.sportsfreunde.de
Torfreunde	www.torfreunde.de/tf/
Yourteam	yourteam.de
Studenten	
Campux	www.campux.com
Nur Studenten	nurstudenten.de
Students	www.students.de
Studentum	www.studentum.de
Studi	studi.net
StudiVZ	www.studivz.net
Studylounge	studylounge.de
Studymee	studymee.com
Unister	www.unister.de
Wohnen, Essen, Wein	
Mycellar	www.mycellar.de
Mynesto	mynesto.com
Qype	www.qype.com
So leb' ich	www.solebich.de
Verkostet	www.verkostet.de
Zimmerschau	www.zimmerschau.de/homepage

Onlinequellen

[a] Europäischer Vergleich von Social-Network-Nutzung
www.comscore.com/press/release.asp?press=1801

[b] Ranking von 149 Social Networks in Deutschland
netzwertig.com/2008/04/15/zn-aktuelles-ranking-149-social-networks-aus-deutschland/

[c] Überblick über 100 Social Networks aus Deutschland
netzwertig.com/2007/10/16/zn-uber-100-social-networks-aus-deutschland/

[d] AGOF-Ranking Soziale Netzwerke
www.deutsche-startups.de/2008/06/26/die-groessten-communitys-und-netzwerke-im-agof-ranking/

[e] Google Trends
www.google.de/trends

[f] 175 Internet-Communities
fudder.de/artikel/2008/04/09/175-internet-communitys/

[g] Howard Rheingolds „Virtual Community“
www.rheingold.com/vc/book/

eigene Plattform, damit sie zielgruppengerechte Anzeigen platzieren. Das wiederum erfordert viele, viele Nutzer. Nur bei einem anstehenden Umzug der nutzergenerierten Daten – des viel zitierten UGC (User Generated Content) – guckt der gemeine Anwender in die Röhre. Den Abfluss der mühselig erstellten Daten haben viele Betreiber nicht vorgesehen. (hb)

RAMON WARTALA

ist IT-Leiter beim Hamburger Online-vermarkter orangemedia.de GmbH und Koautor des 2007 bei Addison-Wesley erschienenen „Webanwendungen mit Ruby on Rails“.







Wie Web 2.0 den automatisierten Missbrauch ermöglicht

Schnapp mich

Dominik Birk, Felix Gröbert, Christoph Wegener

Wo immer Daten in großem Ausmaß gesammelt werden, besteht die Gefahr des Missbrauchs. Das gilt auch für Anbieter sogenannter Social Networks à la Xing, StudiVZ & Co. Dort hinterlassen Nutzer freiwillig persönliche Daten in rauen Mengen – zusammen mit technischen Schwachstellen eine gefährliche Kombination.

Das Phänomen des sozialen Netzwerks, das eigentlich aus der Ethnosoziologie stammt, schwappte in den letzten Jahren im Zuge von „Web 2.0“ auch in die virtuelle Welt des Internet über. Für fast jede Zielgruppe gibt es bereits ein eigenes soziales Netzwerk: StudiVZ für Studenten, Xing für Berufstätige – und sogar Hacker machen ihr Open-Source-Engagement auf Plattformen wie „House of Hackers“ und anderen öffentlich (diese und andere Internetquellen zum Artikel sind über den *iX*-Link zu finden).

Die eigentliche Informationsbasis in sozialen Netzwerken sind die Profile der Nutzer, denn sie enthalten alle relevanten Daten. Dazu gehören neben soziodemografischen Daten wie Namen, Alter, Geburtsdatum und Adresse auch spezielle (persönliche) Merkmale wie die politische Gesinnung oder Vorlieben für Nahrungsmittel und Sportarten.

Jedoch hat das Veröffentlichen von persönlichen Attributen in sozialen Netzwerken zwei Seiten: Einerseits eröffnet die Herausgabe von Informationen den aktiven Nutzern das komplette Spektrum an Funktionen des Web 2.0 (und das Kontakteknüpfen aufgrund bestimmter Eigenschaften oder Vorlieben ist ja gerade eine Kernfunktion solcher Netzwerke), während Mitglieder, die kaum Informationen über sich selbst publizieren, auch nur bedingt von den Vorteilen profitieren können. Andererseits birgt die freizügige Preisgabe personenbezogener Daten aber immer die Gefahr des Missbrauchs, etwa in Form der unten dargestellten Angriffe. Eine wesentliche Herausforderung für den modernen Nutzer ist es daher, die Balance zwischen „gläsernem“ und „passivem“ Mitglied eines sozialen Netzwerks zu finden (Abb. 1).

Angriffstechniken im Überblick

Da Web-2.0-Anwendungen häufig sämtliche zur Verfügung stehenden Technologien client- und serverseitig voll ausnutzen, bietet sich dem Angreifer ein breites Spektrum an Angriffsmöglichkeiten. Abgesehen von DNS-Manipulationen [a] zum breitangelegten Pharming, also dem (großflächigen) Umleiten von beispielsweise Internetbanking-Kunden auf gefälschte Server, finden die meisten Angriffe auf HTTP-Ebene und darauf aufsetzenden Verfahren statt.

In letzter Zeit häuft sich etwa der Einsatz sogenannter Web-Exploit-Toolkits [b], die Schwachstellen in Browsern und populären Plug-ins ausnutzen. Solche Angriffe haben das Ziel, auf dem Client beliebigen Code auszuführen und ihn in einem zweiten Schritt in ein Botnetz zu integrieren, Adware zu installieren oder beispielsweise Klickbetrug zu betreiben.

Angriffe auf Server können zwar sekundär angebotene Serverdienste ausnutzen, beispielsweise verwundbare SQL-Server oder schwache FTP-Passwörter, jedoch zielen sie meist darauf ab, die primär angebotene Webanwendung anzugreifen. Während die HTTP-Server (Apache, IIS) in der Vergangenheit kaum Memory-Corruption-Schwachstellen aufwiesen, lässt sich, das zeigt unter anderem die Schwachstellendatenbank des NIST, ein deutlicher Anstieg bei den frei angebotenen und quelloffenen Webanwendungen verzeichnen (siehe Tabelle „Schwachstellen in Webanwen-

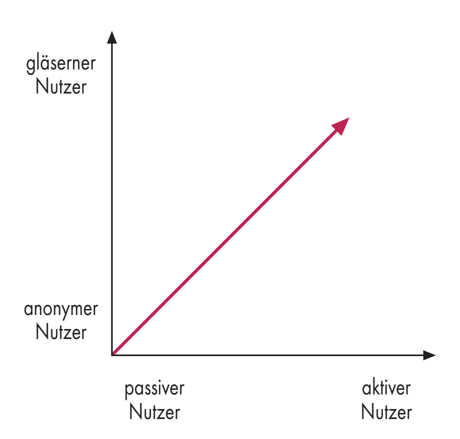
dungen“). Typische Angriffe auf Webanwendungen beschreibt der gleichnamige Kasten. Zudem darf auch der bedeutende Anstieg von bekannt gewordenen Schwachstellen in Interpreter-Sprachen wie Ruby, PHP oder Python nicht unterschätzt werden.

Durch soziale Netzwerke kann man die Anzahl der Opfer von Webangriffen auf einen Schlag wesentlich erhöhen. Eine mathematische Betrachtung verdeutlicht die Dimension des Problems.

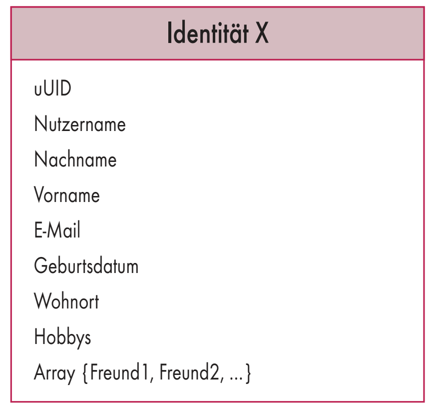
Soziale Netzwerke kann man als Graphen darstellen, aufgebaut aus Knoten und Kanten. Ein Knoten steht als Repräsentant für eine Identität und besitzt spezifische Attribute, zum Beispiel Name, Vorname, E-Mail-Adresse et cetera. Eine Kante hingegen, die zwei Knoten miteinander verbindet, stellt die Relation zwischen diesen dar. Zusätzlich kann diese Kante mit einem Wert versehen sein, um die Stärke der Beziehung zu definieren – was sich bei sozialen Netzwerken im Internet aber als recht schwierig herausstellt.

Von letztgenannter Einschränkung abgesehen, ist dieses Modell ideal für eine maschinelle Datensammlung und -speicherung, um Angriffe im großen Stil fahren zu können. Dazu wäre beispielsweise der folgende, in zwei Phasen aufgeteilte Ansatz denkbar. Zunächst zur Aggregationsphase. Eine Identität X wird durch ein Tripel (i, A, R) definiert, wobei i eine eindeutige Kennziffer dieser Identität (uUID), A die Menge aller persönlichen Attribute a und R die Menge aller Relationen r zu anderen Identitäten ist. Ein Angreifer sammelt zunächst breit angelegt identitätsbezogene Profilinformationen und -relationen aus mehreren sozialen Netzwerken und speichert sie in den Identitätstripeln. Das Profil einer solchen Identität X könnte wie in Abbildung 2 aussehen.

Die Profilaggregation von Nutzerdaten fällt dem Angreifer auf vielen Plattformen leicht, da diese in der Regel keinerlei Schutzmaßnahmen, etwa gegen automatisierte Crawler, einsetzen und die Profile kaum unter Datenschutzaspekten ausgestaltet sind. Manche soziale Netzwerke ermöglichen gar, dass die Nutzer-ID per GET übergeben wird, also in der Form http://…?id=1234. Ein Angreifer kann so nach und nach alle Werte für IDs durchprobieren. Turing-Tests, die zwischen automatisierten und manuellen Eingaben unterscheiden sollen, sind heutigen Angriffen häufig hilflos ausgeliefert – so stellen klassische Captchas kaum noch eine Hürde für rechnergestützte Attacken dar [1].



Zu wenig Informationspreisgabe schränkt Vorteile und Funktionen des Internet ein, zu viel birgt die Gefahr des Missbrauchs und des „gläsernen Menschen“. Gefragt ist ein guter Mittelweg (Abb. 1).



Vor allen anderen Schritten sammelt ein Angreifer so viele Identitäten wie möglich. Diese definieren sich durch eine eindeutige Kennung, individuelle Attribute sowie ihre Beziehungen zu anderen Identitäten (Abb. 2).

Strukturierte Daten vereinfachen Missbrauch

Gerade die einheitliche Darstellungsstruktur in sozialen Netzwerken erleichtert das Crawlen der Daten. Während im „Web 1.0“ wenige Nutzer die Informationen für viele Nutzer in unterschiedlichsten Datenstrukturen publizierten, hat sich mit dem Web 2.0 das Blatt gewendet: Jeder kann multimediale Inhalte für die große Internetgemeinschaft liefern. Diese Inhalte liegen, so will es die Plattform, in einer bestimmten Struktur vor, wodurch es für einen Crawler umso einfacher ist, die Semantik der vorgefundenen Daten zu bestimmen.

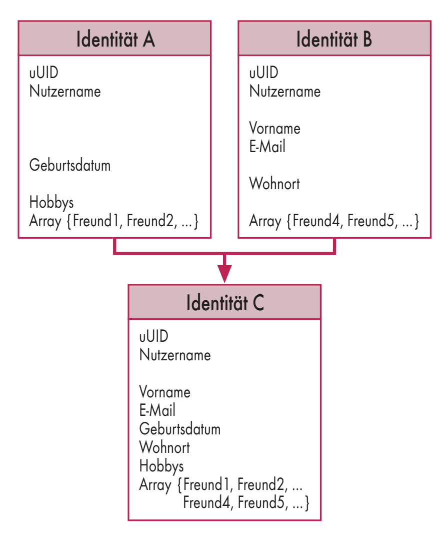
In der zweiten, der Korrelationsphase, versucht der Angreifer nun, Profilkorrelationen zwischen den Identitäten verschiedener Netzwerke herzustellen. Das ist häufig möglich, denn meist nutzt ein Internetnutzer gleich mehrere Web-2.0-Anwendungen parallel. Auf der einen Plattform speichert er seine persönlichen Bilder, auf der nächsten betreibt er sein eigenes Weblog und auf der dritten pflegt er schließlich die Kontakte zu Freunden, Bekannten und Arbeitskollegen.

Korrelationen lassen sich nun durch Übereinstimmungen oder Ähnlichkeiten verschiedener Profilattribute und gegenseitig verweisende Relationen herstellen. Des Weiteren können Data-Mining-Methoden für Graphen dazu benutzt werden, bekannte soziale Topografien einer Identität eines sozialen Netzwerks in einem anderen Netzwerk zu suchen. Diese Methoden lassen sich beispielsweise gut anwenden, sobald der Verdacht besteht, dass es sich bei zwei Identitäten in zwei Netzwerken um ein und dieselbe reale Person handelt.

Für den Angriff ist es prinzipiell egal, wie stark eine Relation zwischen zwei Identitäten definiert wird, Hauptsache sie besteht. Die Kenntnis dieser Stärke kann für den Angreifer dennoch von Vorteil sein, da sie ihm Informationen über besonders lohnenswerte Ziele, das heißt Identitäten mit starken Relationen, liefern kann.

iX-TRACT

- Nutzer geben in sozialen Netzwerken häufig so zahlreiche Informationen über sich und ihre Vorlieben preis, dass potenzielle Angreifer sie leicht überlisten und ihnen beispielsweise Phishing-Nachrichten erfolgreich unterjubeln können.
- Da solche Plattformen alle Daten in einer strukturierten Form vorhalten, lassen sich etliche dieser Angriffe automatisiert durchführen.
- Besonders gefährlich ist die Ausnutzung menschlicher Gutgläubigkeit in Kombination mit den technischen Angriffsmöglichkeiten.



Da viele Internetnutzer mehrere Webanwendungen benutzen, lassen sich häufig deren Daten anhand von Übereinstimmungen in Benutzernamen, Vorlieben et cetera korrelieren – das Wissen über sie wächst ... (Abb. 3).

Daneben existieren noch weitere Möglichkeiten für die Aggregation von Daten:

– Die Motivation für den Angriff auf die Privatsphäre der Kunden kann auch von innen kommen. Der Angreifer hat als Insider – wie jüngst bei der Telekom – dann bereits vollen Zugriff auf alle Daten.

– Unternehmen und Daten können verkauft werden. Problem hier: Rechte und Pflichten für personenbezogene Daten sind international sehr unterschiedlich ausgeprägt. Ein Missbrauch der Daten wird zudem – absichtlich oder unabsichtlich – durch den Verkauf oder die Weitergabe an Dritte ermöglicht.

– Personenbezogene Daten können darüber hinaus durch realen und digitalen Diebstahl verloren gehen. Dass solche Einbrüche häufig geschehen, zeigt das Projekt „DataLossDB“ (siehe *iX*-Link), das alle bekannt gewordenen Datenverluste sammelt und veröffentlicht. Allein für das Jahre 2008 sind dort 149 Vorfällen verzeichnet, bei denen verschiedene personenbezogene Daten von über 25,1 Mio. Personen gestohlen wurden (Stand: 29. Juni 2008).

– Bereits bestehende Profile können mit Suchmaschinen und sogenannten „Personensuchmaschinen“ verifiziert, verknüpft und weiter vervollständigt werden (Abb. 3).

Wer wird das Opfer?

Diese Phase ist für den Angreifer aber in den meisten Fällen optional, da sie lediglich zur Profilvervollständigung beiträgt und viele soziale Netzwerke bereits

Wie soziale Netzwerke die Unternehmenssicherheit bedrohen können

Neben den im Artikel beschriebenen mathematisch fundierten, automatisierten Angriffen gegen die Benutzer von Social Networks laden diese auch zum klassischen Social Engineering ein. Denn das, was Nutzer in solchen Netzwerke bezwecken, lässt sich nur mit der Preisgabe persönlicher Daten erreichen. In der Regel sind das Name und Vorname plus Foto. Wenn jemand beispielsweise Mitschüler sucht, geht es nicht ohne solche Informationen.

Für geschäftliche Interessen von Teilnehmern sind weitere Angaben wie E-Mail-Adresse, Geburtsdatum, Wohnort und Ausbildung, geschäftliche Auskünfte wie Werdegang, Arbeitgeber und Position sowie Nennung persönlicher Interessen von Vorteil. Das Problem ist offensichtlich. Der Teilnehmer hinterlässt mit diesen Informationen seine Datenspuren in einem öffentlichen Netzwerk, auf deren Verbreitung er im Weiteren keinen Einfluss mehr hat.

Angreifer können sich zunächst solcher Informationen bedienen, um sich ein Bild ihres Opfers zu machen. Ihr Ziel ist es, die Sicherheitsmechanismen eines Unternehmens zu umgehen und an vertrauliche Daten zu gelangen. Vielen Community-Teilnehmern ist nicht klar, dass solche nicht nur aus Passwörtern oder einbruchsrelevanten Informationen et cetera bestehen. Schon ein Adressbuch eines Beraters kann als vertraulich eingestuft werden, denn sollte ein Konkurrent darauf Zugriff erhalten, kann das ernsthafte Auswirkungen auf die Zukunft des Beraters haben.

Wie „Social Hacker“ vorgehen

Teilnehmer an sozialen Netzwerken sind sich oftmals kaum bewusst, dass sie ein ideales Angriffsziel für sogenannte „Social Hacker“ sind – also Angreifer, die vorwiegend mit Techniken des Social Engineering arbeiten (zahlreiche Internetquellen zu Social Engineering sind über den *iX*-Link zu finden).

Ziel dieser Techniken ist zunächst nicht der direkte Einbruch in ein IT-System, sondern das Erlangen vertraulicher Informationen. Hierzu greift der Social Hacker keine Firewall und kein Intrusion-Detection-System an, sondern das schwächste Glied in der IT-Sicherheit, den Menschen. Er wendet psychologische Tricks an, um sein Opfer dazu zu bringen, zu tun, was er verlangt. Damit das gelingt, ist es wichtig, dass er das Vertrauen seines Opfers erlangt, um es später beliebig manipulieren zu können.

Der Angreifer macht sich die natürliche Tendenz von Menschen zunutze, anderen ihr Vertrauen zu schenken. Dies gelingt am besten, wenn er möglichst viele private und auch geschäftliche Details über das Opfer weiß. Daten, die ihm eventuell schon auf der jeweiligen Profilseite auf dem Silbertablett präsentiert werden. Beim Social Engeneering gilt: Je mehr Informationen der Angreifer hat, desto einfacher ist es, sich das Vertrauen des Opfers zu erschleichen.

Welche dramatischen Auswirkungen solche Täuschungen haben können, zeigt der Fall der 13-jährigen Megan Meier aus Missouri, die sich im Oktober 2006 nach einem Streit mit ihrem vermeintlichen Onlinefreund von Myspace das Leben nahm. Wie sich im Nachhinein herausstellte, steckte hinter der Identität des Onlinefreundes in Wirklichkeit eine gekränkte Freundin aus der Nachbarschaft.

Unzureichende Schutzmaßnahmen

In vielen Communities gibt es einen Basis-Sicherheitsmechanismus. Die Allgemeinheit der Community-Mitglieder hat nur rudimentären Zugriff auf die Profilseiten anderer Mitglieder, kann also nur grundlegende Daten wie Name, Nachname, Foto und die abonnierten Gruppenmitgliedschaften einsehen. Nur als Kontakt akzeptierte Mitglieder – man spricht vom eigenen Netzwerk – können weitergehende Informationen aus dem Profil sehen, zum Beispiel die Liste der eigenen Kontakte.

Diese Schutzfunktion ist beim Erstellen einer Profilseite meistens nicht standardmäßig aktiviert. Recherchen zeigen im Gegenteil, dass sie kaum genutzt wird. Außerdem bringt sie nur etwas, wenn man seine Kontakte sehr bewusst auswählt und nicht gleich jede Kontaktanfrage blindlings akzeptiert. Aber auch hier ist genau das Gegenteil zu beobachten. Viele Teilnehmer in Communities scheinen geradezu besessen nach Kontakten zu sein und versuchen mehr oder weniger grundlos, ein möglichst großes Kontaktnetz zu knüpfen.

Doch selbst von einem wachsamen Community-Teilnehmer lässt sich ein ernsthafter Angreifer kaum aufhalten. Er sucht in den Diskussionsforen nach fachlichen Beiträgen des Opfers und geht auf sie ein. Auf diese Weise kann er das Vertrauen seines Opfers gewinnen und sicherlich bald in dessen persönliches Netzwerk aufgenommen werden.

Mehr Kontakte, mehr Informationen

Hat der Angreifer Einsicht in die weiteren Kontakte des Opfers, wird er das nutzen, um auch diese näher kennenzulernen. Eventuell kann er die neu erworbene Beziehung zum Opfer sogar nutzen, um auch in das Netzwerk der primären Kontakte des Opfers aufgenommen zu werden. Das Opfer dient quasi als Leumund.

Hat der Angreifer das Netzwerk des Opfers ausgiebig analysiert, wird er auch in alternativen Communities sowie allgemein im Internet nach weiteren Informationen über sein Opfer sowie dessen Kontakte suchen. Suchmaschinen liefern hier Informationen, ebenso kommerzielle Seiten wie Ebay und Amazon oder Personensuchmaschinen wie www.yasni.de oder www.spock.com, die auch gleich weitere Communities überprüfen.

Sicherlich ist das eine Fleißarbeit, die aber in vielen Fällen reichlich belohnt wird. Der Angreifer kann auf interessante Details stoßen, zum Beispiel auf private Webseiten oder Blogs, private Fotos, fachliche Texte aus dem geschäftlichen Umfeld, weitere private oder geschäftliche E-Mail-Adressen, in welchen Vereinen das Opfer Mitglied ist, Postings von Familienangehörigen und so weiter.

Erst sammeln, dann angreifen

Ab diesem Zeitpunkt hat der Angreifer genug Informationen, um einen erfolgreichen Angriff zu starten. Zunächst kann er versuchen, mit den vorhandenen Informationen das Passwort zu einem der gefundenen Accounts zu erraten. Gelingt es ihm, stehen die Chancen nicht schlecht, dass dieses Passwort auch bei anderen Zugängen, zum Beispiel einem Remote-Zugang zum Unternehmen genutzt wird.

Einfacher wäre es aber, eine gespoofte E-Mail an das Opfer zu senden. Nicht nur die Mail-Adressen, sondern auch die Beziehungen von Freunden und Kontakten des Opfers sind dem Angreifer zu diesem Zeitpunkt ja schon bekannt. So wird es ihm nicht schwerfallen, einen kleinen authentischen Text zu erstellen und eines der gefundenen Fotos anzuhängen. Das Foto wurde vorher mit Malware, beispielsweise einem Trojaner infiziert, natürlich einem, den kein Virenscanner erkennt. Trojanerbaukästen dieser Art gibt es im Internet zu kaufen. Alternativ könnte der Angreifer auch seine eigene Profilseite mit verseuchten Elementen versehen. Dieses Szenario eignet sich jedoch besser für einen ungezielten Angriff auf möglichst viele Opfer.

In beiden Szenarien hat das Opfer kaum eine Chance, den Angriff direkt zu erkennen – es sei denn, die Kommunikation mit Kontakten und Bekannten erfolgt immer mit kryptografischen Verfahren wie der digitalen Signatur.

Aber warum überhaupt eine E-Mail-Adresse eines Bekannten spoofen und nicht gleich eine neue Mail-Adresse in dessen Namen anlegen, also sozusagen seine Identität spoofen? So hätte der Angreifer

Fortsetzung Seite 50

genügend Informationen preisgeben, um ein Identitätsprofil anschaulich auszufüllen. Zudem handelt es sich dabei häufig um ein zeit- beziehungsweise rechenintensives Verfahren.

Bei der hier vorgestellten Angriffsmethode macht der Angreifer sich die sogenannte „Trusted Relation“ zwischen zwei Identitäten innerhalb eines Netzwerkes zunutze, indem er sich in betrügerischer Weise für eine Identität ausgibt und anschließend die zweite im Namen dieser kontaktiert. Studien haben ergeben, dass rund 36 % der Nutzer von sozialen Netzwerken den Nachrichten von Freunden oder Bekannten innerhalb des gleichen Netzwerkes absolut vertrauen.

Angenommen, ein Angreifer ist bereits im Besitz von Profilen inklusive Relationen aus einem Teilbereich eines sozialen Netzwerkes. Der Informationsgrad einer Identität (deg) lässt sich wie folgt beschreiben: deg(a,r) = Summe a + Summe r. a repräsentiert die verfügbaren persönlichen Attribute und r die gesammelten Relationen, die eine Identität besitzt. Dem Angreifer ist es nun möglich, das komplette soziale Netzwerk eines Graphen G (oder Teile davon) in einem Teilgraphen H in Form eines Soziogramms darzustellen. Soziogramme sind in dem Fall ebenfalls mathematische Graphen, allerdings solche, die speziell für soziologische Zwecke genutzt werden können [c].

Um aus diesem Teilgraphen H nun potenzielle Opfer zu finden, stehen einem Angreifer wiederum verschiedene Möglichkeiten zur Verfügung, von denen hier nur einige genannt werden:

– Eine potenzielle Opfergruppe sind Identitäten mit einem möglichst hohen Informationsgrad. Das bedeutet, dass über diese Identitäten sowohl eine Menge persönliche Attribute als auch Relationen zu anderen Identitäten verfügbar sind. Ein Angreifer könnte so gezielt die verfügbaren Attribute und Relationen dazu benutzen, das Opfer anzulocken.

– Des Weiteren könnte der Angreifer nach sogenannten „Brokers“ im Teil-

Typische Angriffe auf Webanwendungen

Nicht-persistentes und persistentes Cross-Site Scripting (XSS): Hier injiziert der Angreifer HTML und/oder Javascript temporär oder persistent in eine Seite. Das Opfer bekommt beispielsweise eine falsche Meldung angezeigt oder die Zugangsdaten für die Seite werden gestohlen.

Beispiel-Angriffscode:

```
"><script>alert(1);</script>
```

Cross-Site Request Forgery (XSRF): Das Opfer sendet unwissentlich ein Formular an seine Webanwendung, indem es eine bösartige Seite besucht. Dass die Webanwendung dieses Formular trotzdem akzeptiert und interpretiert, lässt auf einen XSRF-Fehler schließen.

Beispiel-Angriffscode auf fremder Webseite:

```
<body onload="document.attack.submit();">
<form action="http://example.com/addBuddy" ↲
                    method="POST" name="attack">
<input name="Buddy" value="Some ↲
                                   Dude"></form>
```

SQL Injection (SQLi): Benutzereingaben, beispielsweise bei einem Login, werden von der Webanwendung unzureichend geprüft und an den SQL-Server weitergegeben. Der Angreifer kann nun die SQL-Befehle an den Server ändern und sich beispielsweise [e] als beliebiger Benutzer anmelden, ohne das Passwort zu kennen.

Beispiel-Angriffscode für Injection von MySQL-Kommentaren (--):

```
 Login: Opfer " -- "
 Passwort: Unbekannt!111!elf
 SQL Query: SELECT [...] WHERE
`Identity`.`username` = "Opfer" -- "" ↲
                 AND `Identity`.`password` = [...]
```

OS Command Injection: Wie SQL Injection, nur werden Befehle an eine Shell des Betriebssystems gegeben.

Beispiel-Angriff zur Injection von OS-Befehlen:

```
Benutzereingabe: 13:45 ; rm -rf /
OS Befehl: date -s 13:45 ; rm -rf /
```

HTTP Response Splitting: Wie XSS, nur kann der Angreifer Daten im HTTP-Header des verwundbaren Servers ändern, um beispielsweise einen „302 Redirect“ zu fälschen.

Remote File Inclusion (RFI): Bei Webanwendungen, die auf serverseitigen Skriptsprachen basieren, können Dateien von entfernten Webservern in die Webanwendungen geladen und interpretiert werden.

Wie Soziale Netzwerke die Unternehmenssicherheit bedrohen können (Fortsetzung)

gar die Möglichkeit zur bidirektionalen Kommunikation.

Identitätsdiebstahl, „Identity Theft“, assoziiert man zurzeit vorrangig mit Kreditkartendaten und dem Verlust von Geld vom eigenen Konto ins Ausland. Web 2.0 aber bietet völlig neue Anwendungsmöglichkeiten für diese Art der Kriminalität.

Die Wurzel des Übels liegt bei der Identifikation/Authentifizierung. Diese findet zwar auf Systemebene statt, aber eben nur dort. Man kann derzeit nicht feststellen, ob ein Community-Profil auch wirklich zu der realen Person gehört. Dies muss schon „Out-of-Band“ erfolgen, zum Beispiel durch persönliches Nachfragen. Ein Alptraum in Sachen Sicherheit, ein Traum für jeden Social Hacker.

Der böse Zwilling

So kann ein geschickter Angreifer in einer Community gleich die ganze Identität einer dritten Person übernehmen und in deren Namen ein gefälschtes Profil erstellen. Mit den bei der Recherche gefundenen Daten wie Namen und Foto lässt sich innerhalb kurzer Zeit eine glaubhafte Profilseite erstellen – der Evil Twin. Dass es sich hier um eine Fälschung handelt, ist auf den ersten Blick nicht zu erkennen.

Der Angreifer wird also vorrangig eine Person mimen, die geschäftlich reizvoll für das Opfer ist. Sollte der Angriff nur eine kurze Zeit andauern, kann er eine Person aus dem direkten Umfeld wie einen Vorgesetzten oder einen Arbeitskollegen darstellen. In anderen Fällen könnte es ein interessierter Kunde oder ein Headhunter auf der Suche nach qualifiziertem Personal sein.

Gerade beim Verkörpern wichtiger Persönlichkeiten kann der Informationsgewinn immens sein. Das hat vor allem psychologische Gründe. Angenommen, ein (vermeintlicher) Direktor eines größeren Unternehmens akzeptiert einige „kleine“ Angestellte einer Community in seinem persönlichen Netzwerk. Das würde für die betroffenen Kollegen einen großen Akzeptanzgewinn im Unternehmen bedeuten und könnte sich nach deren Meinung positiv auf ihre Karriere auswirken. Sicherlich ließen sich über sie vertrauliche Insider-Informationen aus dem Unternehmen erhalten.

Um in der Praxis – ohne jemandem Schaden zuzufügen – auszuprobieren, wie einfach die Kontaktaufnahme ist, übernahm der Autor kurzerhand die Identität von Ludwig van Beethoven. Bereits kurze Zeit nach Erstellung der Profilseite lagen vier Einladungen von dem Autor völlig unbekannten Personen vor.

Neben dem Versuch des Informationsdiebstahls kann der Evil Twin auch dazu missbraucht werden, durch Falschaussagen, unflätige oder dumme Postings ein schlechtes Licht auf andere zu werfen. Hierbei wirkt das psychologische Moment, das Menschen dazu neigen, ungeprüft alles zu glauben, was sie irgendwo lesen. Ein negatives Urteil wird dem Opfer unweigerlich nachhängen, denn kaum ein Personalberater oder potenzieller Geschäftspartner wird sich die Mühe machen, die Echtheit solcher Informationen zu überprüfen.

Wie man sich schützt

Zuallererst sollte man darauf achten, private sowie geschäftliche Daten auch wirklich privat zu halten und nicht öffentlich verfügbar zu machen. Zugegebenermaßen erfordert dies je nach Situation ein großes Maß an Disziplin. Dennoch: Wie verlockend ein Kontakt-, Dienste- oder anderweitiges Angebot im Internet auch klingen mag, man sollte nicht versäumen, Angebot wie Anbieter gründlich zu durchleuchten.

Mit der Preisgabe von Informationen auf Profilseiten und Diskussionsforen sollten Internetnutzer vorsichtig und sparsam umgehen, und auch beim Knüpfen von Kontakten ein gesundes Maß an Vorsicht walten lassen. Selbst wenn man alles richtig macht, kann ein Angriff niemals ganz ausgeschlossen werden. Aber man wird ihn zumindest schneller als solchen erkennen – vielleicht bevor es zu spät ist. *Michael Hamm*

So könnte ein Angriff aussehen

Ein Konkurrent will Kontaktdaten von Kunden aus einem Unternehmen stehlen. Die Mitarbeiter des Unternehmens sind sehr vorsichtig in der Community und nutzen alle Sicherheitseinstellungen.

1. Der Angreifer sucht allgemein via Internet nach Namen von Mitarbeitern des Unternehmens. –> Er findet 10 gültige Namen.

2. Der Angreifer recherchiert in Business-Netzwerken wie Xing und Linkedin nach Profilen von Mitarbeitern des Unternehmens. –> Er findet 4 Profilseiten von Mitarbeitern. –> Er findet 1 Profilseite eines ehemaligen Mitarbeiters. –> Er findet diverse Forumsbeiträge, in denen auch die eigenen Produkte beschrieben werden.

3. Der Angreifer konzentriert seine allgemeinen Internetrecherchen auf die fünf gefundenen Personen. –> Er kann die Position von zwei Mitarbeitern im Unternehmen identifizieren.

4. Der Angreifer erstellt eine Profilseite. Er gibt an, Abteilungsleiter eines mittelgroßen Unternehmens zu sein und zeigt Interesse an den Produkten des Unternehmens. –> Ein Mitarbeiter des Unternehmens akzeptiert den Angreifer als neuen Kontakt.

5. Der Angreifer hat nun Zugriff auf das soziale Netzwerk des Mitarbeiters und durchforscht es gründlich. –> Er stellt fest, dass es zwei weitere ehemalige Mitarbeiter gibt, die aber offensichtlich noch keine Profilseite haben.

6. Er forscht im Internet nach diesen ehemaligen Mitarbeitern. –> Ein ehemaliger Mitarbeiter nimmt aktiv am örtlichen Karnevalsverein teil. –> Es ist reichlich Bildmaterial vorhanden.

7. Mit einem der Bilder erstellt der Angreifer eine neue Profilseite im Namen des Ex-Kollegen.

8. Der Angreifer nimmt Kontakt mit dem ersten ehemaligen Mitarbeiter auf. –> Dieser akzeptiert ihn sofort. –> Beide tauschen sich ein wenig aus.

9. Der Angreifer kennt genug Fakten. –> Der ehemalige Mitarbeiter schöpft nicht den geringsten Verdacht. –> Auch über ehemalige Projekte und Kontaktdaten von Kunden wird endlich gesprochen.

10. Parallel dazu hat der Angreifer den Kontakt mit dem Mitarbeiter ausgebaut, bittet um ein erstes nicht offizielles Angebot und bietet ein Treffen an. –> Der Mitarbeiter bittet um eine kurze Anforderungsbeschreibung.

11. Der Angreifer kopiert eine Anforderungsbeschreibung aus dem Internet, erstellt eine PDF-Datei und infiziert sie mit einem „neuen“ Trojaner. –> Der Empfänger öffnet die Datei. –> Der Trojaner startet eine Back Connect Shell zu einem vom Angreifer übernommenen System in Taiwan. –> Der Virenscanner erkennt den neuen Trojaner nicht. –> Die Firewall erlaubt die ausgehende Verbindung zu Port 80. –> Da der Mitarbeiter auf seinem System mit Administratorrechten arbeitet, hat der Angreifer vollen Zugriff auf das System.

MICHAEL HAMM

ist Ingénieur Sécurité am Centre de Recherche Public Henri Tudor in Luxemburg.

graphen H suchen. Den Begriff „Broker“ in sozialen Netzwerken beschreibt Valdis E. Krebs in seiner Arbeit „Uncloaking Terrorist Networks“ [d]. Er ist eine Person in einem sozialen Geflecht, die als Bindeglied zwischen zwei Identitäten oder Teilgraphen fungiert. Diese Identität spielt also eine bedeutende Rolle in einem Teilgraphen oder einem Teil davon, daher kann man davon ausgehen, dass der dieser Identität zugehörige Informationsgrad in Bezug auf bestehende Relationen recht hoch ist. Man spricht in der Graphentheorie auch von einer ausgeprägten „Nachbarschaft“ eines spezifischen Knotens.

– Der Cluster-Koeffizient eines Knotens beziehungsweise einer Identität beschreibt, wie nah die Identität und ihre relativen Identitäten an einen vollständigen Graphen heranreichen. Ein vollständiger Graph, also einer, bei dem alle relativen Identitäten einer Identität untereinander verbunden sind, besitzt somit den höchsten Cluster-Koeffizienten. Hohe Cluster-Koeffizienten sagen sehr viel über die Relationen des Umfeldes einer Kernidentität aus. Die Berechnung des Cluster-Koeffizienten von Kernidentitäten kann einem Angreifer somit eine Aussage liefern, inwieweit auch das Umfeld der Kernidentität gut angreifbar ist.

Ein Zusammenspiel dieser drei Methoden kann die Suche nach Opfern noch effizienter gestalten, da etwa speziell nach bestimmten Opfergruppen mit möglichst hohem Informationsgrad, einem eventuell vorhandenen Broker und einem möglichst maximalen Cluster-Koeffizienten gesucht werden kann.

Der Angriff kann beginnen

Aus dem oben genannten Teilgraphen H selektiert ein Angreifer nun entsprechende Opfer. Dabei gilt folgendes Prinzip: Je mehr sich die Identitätstripel im Teilgraphen H vervollständigen lassen, desto höher die Wahrscheinlichkeit einer erfolgreichen Attacke.

Der eigentliche Angriff sieht im Vergleich zu den vorhergehenden Verfahren recht primitiv aus. Angenommen, es gibt eine Identität U, einen Broker mit geringem Cluster-Koeffizienten, der jedoch Relationen zu Identität V, W, X, Y und Z pflegt, deren Informationsgrad in Hinsicht auf die persönlichen Attribute recht hoch ist.

Der Angreifer startet nun eine sogenannte Spear-Phishing-Attacke auf Identität V, W, X, Y und Z, indem er ihnen Phishing-Nachrichten im Namen von Identität U schickt. Wichtig ist hierbei, dass personifizierte Merkmale in der Nachricht auftauchen, die der

Schwachstellen in Webanwendungen

Kategorie	Anteil an allen CVEs 2008
SQL Injection	18 %
XSS	16 %
Buffer Errors	12 %
Format String Bugs	1 %

Schwachstellen in Webanwendungen haben in den vergangenen Jahren deutlich zugelegt. Die Tabelle, die auf der CVE-Datenbank (CVE, Common Vulnerabilities and Exposures) des NIST mit Stand vom 15. Juni 2008 beruht, zeigt ihren Anteil an den gesamten Schwachstellen.

Angreifer aufgrund seiner sozialen Netzwerkanalyse gewinnen konnte. Eine Nachricht könnte beispielsweise wie folgt aussehen:

Hallo $Identität-[V|W|X|Y|Z].Vorname,

ich bin durch Zufall auf folgendes Onlineangebot <bösartiger Link> gestoßen und dachte mir, dass Dich das interessieren könnte, da Du Dich ja auch für $Identität-U.Attribut-1 und $Identität-U.Attribut-2 interessierst. Wie geht es eigentlich $Identität-U. Relation-1?

Ich hoffe, wir sehen uns bald mal wieder beim $Identität-U.Attribut-3.

Viele Grüße, Dein Kumpel $Identität-U.Vorname

Natürlich lassen sich solche Angriffe vollständig anpassen und aufgrund der gleichen Struktur hervorragend automatisieren. Wenn der Angreifer beispielsweise noch die Information besitzt, dass Identität W eine Relation mit Identität Z besitzt, könnte er in seiner Nachricht an Identität W noch den Namen von Identität Z erwähnen, was das Vertrauensverhältnis weiter bekräftigen würde. Je mehr bekannte Merkmale Identität W beim Lesen der Nachricht auffallen, desto höher ist die Chance, dass sie auf die Phishing-Nachricht hereinfällt und den bösartigen Link besucht. Auch lassen sich Nachrichten durch technische Schwachstellen wie XSS authentischer konstruieren.

Die Vergangenheit hat zudem gezeigt, dass der Mensch sich gerne durch vorgespielte Tatsachen in Phishing-Nachrichten täuschen oder beeindrucken lässt. Beispielsweise ging der Trend von der einfachen Phishing-E-Mail, in welche das Opfer zur Eingabe ihrer persönlichen Informationen gebeten wurde, über zu E-Mails, die das Opfer zur Preisgabe nötigten (indem etwa mit Kündigung oder Strafe gedroht wurde).

Angriffe, die sich sowohl technische Schwachstellen als auch das Wissen um das soziale Gefüge der Opfer zunutze machen, sind besonders gefährlich und Erfolg versprechend. Aufgrund der massiven Benutzerzahlen von Web-2.0-Anwendungen reicht es für viele Angreifer schon aus, wenn nur ein kleiner Prozentsatz auf den Angriff hereinfällt.

Verhalten je nach Umgebung

Eine der ältesten Erkenntnisse der Sozialwissenschaften ist, dass sich Leute in der Kirche anders verhalten als in der Kneipe, obwohl sie möglicherweise mit denselben Personen zusammen sind. Dass die verschiedenen Identitäten einer einzelnen Person nicht früher schon verknüpft wurden, liegt hauptsächlich daran, dass es im 20. Jahrhundert technisch noch zu aufwendig war.

Heute gibt es diese technische Beschränkung nicht mehr und die unterschiedlichen Identitäten des Kirchen- und Kneipengängers verschmelzen miteinander. Damit sind allerdings auch alle anderen Eigenschaften verbunden, die sich mit der Identität verknüpfen lassen: Attribute, Reputation, Relationen und so weiter.

Für persönliche Daten gibt es vielerlei Missbrauchsmöglichkeiten, zunächst die versehentlich oder beabsichtigt unerwünschte Veröffentlichung durch private oder gar staatliche Stellen zu den verschiedensten Zwecken. Darüber hinaus lassen sich mithilfe der Korrelation von Profildaten auch rasterfahndungsähnliche Methoden umsetzen, zumal auch den Ermittlungsbehörden großes Interesse an diesen Daten nachgesagt wird. Unlängst hat das Pentagon Interesse an den Nutzerprofilen sozialer Netzwerke wie Myspace.com geäußert. Und nicht zuletzt birgt die Veröffentlichung von Daten ein großes ökonomisches Potenzial, das beim Nutzer in Form von (unerwünschter) Werbung wieder ankommt. Angesichts der vorher geschilderten Szenarien ist das aber eher ein harmloses Übel.

Fazit

Ein sicheres Auseinanderhalten der Identitäten bleibt bisher eine noch ungelöste Aufgabe für die einzelnen Nutzer (Verwendung von Pseudonymen, allgemeine Datensparsamkeit, …), für die Technik (Anonymisierungsdienste, …) und für die Gesetzgebung (BDSG, europäische Datenschutzgesetzgebung, …).

Allerdings lassen neue Studien des Wissenschaftszentrums für Sozialforschung in Berlin auf Besserung hoffen: Jüngere Internetnutzer sind sich laut der Studie durchaus der Folgen ihrer hemmungslosen Preisgabe persönlicher Informationen im Internet bewusst. Auch wenn persönliche Datensparsamkeit den Spaßfaktor im Netz unter Umständen etwas ausbremsen kann: Manchmal ist es besser, nicht alle Trends mitzumachen. Oder wie Kryptologe Bruce Schneier es ausdrückt: „Whenever you put data on a computer, you loose some control over it. And when you put it on the internet, you loose a lot of control over it.“ (ur)

DOMINIK BIRK

ist Autor zahlreicher Fachartikel, Gewinner des letztjährigen „Best Student Paper Award“ des BSI und freiberuflich im IT-Sicherheitsumfeld aktiv, derzeit für das spanische VICOMTech-Technologiezentrum in San Sebastian.

FELIX GRÖBERT

ist seit 2003 Student der „Sicherheit in der Informationstechnik“ an der Ruhr-Universität Bochum und freiberuflich in verschiedenen Bereichen der IT und der IT-Sicherheit tätig.

DR. CHRISTOPH WEGENER

ist CISA, CISM und CBP und seit 1999 mit der wecon.it-consulting freiberuflich in den Themen IT-Sicherheit und Open Source/Linux aktiv. Zudem ist er am Horst Görtz Institut für IT-Sicherheit (HGI) in Bochum tätig.

Onlinequellen

- [a] Pharming durch DNS-Manipulation
  www.ngssoftware.com/papers/ThePharmingGuide.pdf
- [b] Web Exploit Toolkits
  www.wecon.net/de/downloads/downloads.html?id=25
- [c] Mukherjee/Holder: Graph-based Data Mining on Social Networks
  users.cs.dal.ca/~eem/malnis/Readings/LinkKDD2004/Maitrayee-Mukherjee-LinkKDD-2004.pdf
- [d] Valdis E. Kreb, Uncloaking Terrorist Networks
  www.firstmonday.org/Issues/issue7_4/krebs/
- [e] SQL-Schwachstelle in NoseRub
  seclog.de/pub/seclog-2007-001.txt

Literatur

[1] Jörn Wagner; Webprogrammierung; Gestaffelte Abwehr; Das Ende der Bild-Captchas; *iX* 4/2008, S. 120







Anwendungen mit der Opensocial-API entwickeln

Anglerlatein

Ramon Wartala

Entwickler, die Anwendungen für die Nutzung in sozialen Netzen planen, wollen nicht mit beliebig vielen Schnittstellen arbeiten. Wenn sie sich auf die Opensocial-API konzentrieren, können sie für eine ganze Reihe von Netzen programmieren.

Die von Google ins Leben gerufene Opensocial-Schnittstelle für die Programmierung von für soziale Netze gedachten Anwendungen kann als Erfolg gelten. Denn mit Orkut, Salesforce.com, LinkedIn, Myspace, StudiVZ und Xing haben bekannte soziale Netze Unterstützung für die API signalisiert. Mittlerweile zählt die Opensocial-Partnerliste an die 80 Firmen (siehe code.google.com/apis/opensocial/partners.html).

Möchte man für soziale Netze der Opensocial-Allianz eigene Anwendungen entwickeln, sind einige Dinge zu beachten. Neben allgemeinen Voraussetzung wie XML-, HTML- und Javascript-Kenntnissen sollte man sich mit der Entwicklung von Webapplikationen beschäftigt haben. Der Artikel in der *iX*-Juliausgabe [1] stellte die Hintergründe und einige Grundlagen zu Googles Opensocial-Programmierschnittstelle dar. Im Folgenden sei die Erstellung einer einfachen Opensocial-Applikation auf Basis einer vorhandenen Webanwendung demonstriert.

Gadgets aus dem Container

Opensocial-Anwendungen nutzen als Rahmen Googles Gadget-API. Gadgets, wie solche Anwendungen heißen, ähneln Portlets: kleine, in sich geschlossene Webkomponenten, die eine Laufzeitumgebung darstellt und ausführt. Opensocial-Gadgets laufen in einer Container-Anwendung, die sich an die Opensocial-Referenz halten muss. Im Rahmen des Apache-Incubator-Projekts Shindig [a] hat Google selbst eine Referenzimplementierung eines Opensocial-Containers als Open-Source-Version veröffentlicht – dazu später mehr.

Opensocial-Gadgets werden durch eine XML-Datei deklariert. Informationen über den Aufbau und Inhalt dieser XML-Datei finden sich in der Gadget-XML-Referenz [b], eine XSD-Schema-Datei liegt unter [c]. Die Struktur der XML-Datei lässt sich grob in fünf Bestandteile gliedern.

1. Metadaten enthalten Informationen über den Autor der Anwendung (E-Mail, URL), den Titel und eine kurze Beschreibung der Applikation.
2. Gadget-Eigenschaften sind Erweiterungen in Form von Javascript-Bibliotheken, die dem Gadget durch Deklaration für den Zugriff zur Verfügung gestellt werden können. So benötigen alle Opensocial-Gadgets die XML-Deklaration

```
<Require feature="opensocial-0.x" />
```

Das „x“ steht für die benötigte Version der API. Ende Dezember 2007 hat Google die Version 0.6 eingeführt, im Januar 2008 schon Version 0.7. Aktuell ist Version 0.8 [d], die Entwickler seit Ende Mai dieses Jahres nutzen können. Leider unterstützen nicht alle Opensocial-konformen Netze jede Version der API.

3. User Preferences sind einfache Schlüssel/Werte-Paare, die Entwickler für die Konfiguration des Opensocial-Gadgets zur Verfügung stellen können, um das Aussehen und das Verhalten zu steuern. Diese Werte speichert der Gadget-Container pro Benutzer. Der Container wiederum stellt in der Regel eine Benutzerschnittstelle für das Editieren dieser Werte zur Verfügung (siehe Listing 1).
4. Message Bundles [e] helfen bei der Entwicklung mehrsprachiger Gadgets. Programmierer, die schon in anderen Programmiersprachen mit Internationalisierung zu tun hatten, dürften dies zu schätzen wissen. Der Mechanismus erlaubt das Anlegen verschiedener Sprachschablonen. Über die Modul-Preferences kann man die jeweilig zu unterstützenden Sprachpakete als XML-Datei importieren (siehe Listing 2). Im HTML-Code des Gadget kann man beispielsweise über *<B>__MSG_color__* auf das Wort „Farbe“ zugreifen.

Listing 1: User Preferences

```
<UserPref
  name="tag_color"
  display_name="TagColor"
  default_value="green"
  datatype="enum" >
  <EnumValue value="green" />
  <EnumValue value="dark green" />
  <EnumValue value="light green" />
</UserPref>
```

Listing 2: Message-Bundle-Einbindung innerhalb einer XML-Datei

```
<ModulePrefs title="test">
  <Locale lang="de" messages="http://doc.examples.
                                    googlepages.com/de_ALL.xml"/>
</ModulePrefs>
```

```
Source View                      Add-ons: co2alarm - OpenSocial   Share
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
  <ModulePrefs
    title="co2alarm - OpenSocial Gadget"
    description=""
    author="Ramon Wartala"
    author_email="ramon@wartala.de"
    author_link="www.wartala.de"
    title_url="co2alarm.homelinux.com"
    author_location="Hamburg, Germany"
    screenshot="http://co2alarm.homelinux.com/images/screenshot.png"
    thumbnail="http://co2alarm.homelinux.com/images/thumbnail.png"
   >
   <Require feature="opensocial-0.7" />
  </ModulePrefs>
  <Content type="html">
        <![CDATA[
        <style type="text/css">
                #gadget {
                        width: 100%;
                        height: 100%;
                        background-color: white;
Save
```

Nicht nur Googles Editor GGE, auch der Opensocial-Gadget-Editor von Webon unterstützt das Erstellen einer Gadget-XML-Datei durch spezielle Eigenschaften (Abb. 1).

5. Der eigentliche Inhalt der Applikation. Dieser kann unter Zuhilfenahme von HTML, CSS und Javascript erzeugt werden.

Auf die einzelnen Inhalte können Entwickler leicht über die von jedem Gadget- und Opensocial-Container zur Verfügung gestellten Javascript-Bibliotheken zugreifen. So ermöglicht die Datei *prefs.js* (zu diesen und anderen siehe die *iX*-Links) den Zugriff auf die Benutzerpräferenzen und die Message Bundles, *io.js* den Zugriff auf entfernte Daten, *json.js* den Umgang mit Daten in der Javascript Object Notation und *util.js* den Zugriff auf Hilfsfunktionen wie dem „Escape“-Markieren von Zeichenketten. Darüber hinaus gibt es eine Reihe weiterer Bibliotheken, die in einem Container zur Verfügung stehen sollten:

tabs.js: erzeugt in der Gadget-Benutzeroberfläche horizontale Reiter zur Navigation über unterschiedliche Inhalte.
minimessage.js: Anzeige einfacher Statusinformationen („lade“ oder „speichere“).
flash.js: Einbau Flash-basierter Inhalte über ein spezielles *embed*-Element.
rpc.js: ermöglicht die Gadget-Container-, Container-Gadget- und Gadget-Gadget-Kommunikation.
views.js: Verwaltung verschiedener Anzeige-Ebenen im Gadget.
skins.js: Abfrage von Farbwerten der Gadget-Umgebung.
dynamic-height.js: ermöglicht dem Gadget, auf seine Vergrößerung oder Verkleinerung zu reagieren.

Was man neben der reinen Funktion bei der Erstellung von Opensocial-Gadgets noch beachten muss, liefern die Guidelines [f].

Wald der Entwicklungswerkzeuge

Zuallererst stellt sich der angehende Opensocial-Entwickler wahrscheinlich die Frage, welche Werkzeuge ihm bei der Erstellung helfen können und welche er davon vielleicht sogar kostenlos nutzen kann. Generell reicht für erste Opensocial-Applikationen schon ein einfacher Texteditor. Tools wie Firebug für Firefox sollten in keinem Webentwickler-Werkzeugkasten fehlen und verrichten bei der Anwendungsentwicklung wertvolle Dienste.

Gerade bei der Erstellung der Gadget-XML-Datei kann es jedoch sinnvoll sein, wenn zumindest Syntax-Highlighting unterstützt wird. Google preist dafür den hauseigenen Gadget Editor (GGE) an [g]. Andere Mitglieder der Opensocial-Allianz ermöglichen ihren Nutzern ebenfalls, Anwendungen zu editieren (Abbildung 1). Editoren mit XML-Unterstützung eignen sich in der Regel jedoch besser, da sie über einen größeren Funktionsumfang verfügen als Googles Webwerkzeug.

Möchte man seine eigene Opensocial-Anwendung, die man vielleicht sogar als Open Source entwickelt, in einem externen Subversion-Repository ablegen und versionieren, bietet sich Google Code an [h]. Selbstverständlich lässt sich ein derartiges Versionsmanagement-Werkzeug auch lokal oder auf der eigenen Webpräsenz betreiben.

Entfernte Inhalte nutzen

Die mächtigste Form eines Opensocial-Gadget ist die Einbindung von Inhalten, die eine schon bestehende Webanwendung liefern kann. Listing 4 zeigt zwei Javascript-Funktionen, die HTML-Daten über eine entfernte URL einlesen und in das Opensocial-Gadget einfügen. In Zeile 5 baut eine *gadgets.io*-Funktion einen Request zusammen, der als Ergebnis einen Text liefern soll. Zusammen mit der Ziel-URL aus Zeile 6 wird in Zeile 7 der HTTP-Request ausgeführt. Das Ergebnis des Request nimmt die Funktion *response()* entgegen und hängt es an das *div*-Element mit der ID *content_div*. Aufgerufen werden die Funktionen über die *gadgets.util*-Funktion *registerOnLoadHandler* in Zeile 16.

iX-TRACT

- Opensocial-Anwendungen können mit den gleichen Mitteln implementiert werden, wie sie auch für normale Webanwendungen genutzt werden.
- Gadgets halten als Rahmen sowohl interne Funktionen als auch den Zugriff auf externe Datenquellen zusammen und ermöglichen der Laufzeitumgebung die Registrierung und Darstellung.
- In Gestalt des Apache-Projekts Shindig steht eine Laufzeitumgebung für PHP und Java im Quellcode bereit, die das lokale Entwickeln von Opensocial-Anwendungen ermöglicht.
- Vorsicht ist beim Betrieb von Opensocial-Gadgets geboten, da soziale Netze leicht mehrere 100 000 Aufrufe pro Tag haben können, was die übliche Serverlast und Datenmengen kleiner Hosting-Angebote schnell erschöpfen kann.

Listing 3: Message-Bundle-Datei de_ALL.xml

```
<messagebundle>
  <msg name="color">Farbe</msg>
  <msg name="red">rot</msg>
  <msg name="green">grün</msg>
  <msg name="blue">blau</msg>
  <msg name="gray">grau</msg>
  <msg name="white">weiß</msg>
  <msg name="black">schwarz</msg>
</messagebundle>
```

Listing 4: Entfernte Inhalte als Gadget-Inhalt

```
1  <script type="text/javascript">
2
3      function getHtml() {
4       var params = {};
5       params[gadgets.io.RequestParameters.CONTENT_TYPE] =
                                  gadgets.io.ContentType.TEXT;
6       var url = "http://localhost:3000/clusterings/gadget/1";
7       gadgets.io.makeRequest(url, response, params);
8     };
9
10    function response(obj) {
11      var str = obj.text;
12      var html =  str;
13      document.getElementById('content_div').innerHTML = html;
14    };
15
16    gadgets.util.registerOnLoadHandler(getHtml);
17  </script>
```



Lokale Testphase: das Opensocial-Gadget *co2alarm* innerhalb des Test-Containers von Shindig (Abb. 2)

Außer reinem Text kann ein Request aus XML, JSON, RSS und ATOM bestehen [i]. Der große Vorteil dieser Art von Gadgets ist, dass sich die aufrufenden Inhalte ohne Opensocial-Container oder Internet-Anbindung entwickeln lassen. So können Entwickler ihre Haus- und Hofsprache für die Erstellung verwenden sowie die geplanten Funktionen im Vorfeld lokal prüfen und mit den vertrauten Werkzeugen arbeiten. Erst in einem nächsten Schritt ist es ratsam, die eigene Webanwendung in den Gadget-Kontext zu überführen. Am schnellsten lässt sich dies sicherlich in eine der verfügbaren Laufzeitumgebungen der jeweiligen sozialen Netze nutzen (siehe die *iX*-Links). Gerade im Hinblick auf eine lokale Entwicklung kann aber das eingangs erwähnte Shindig (engl. für Budenzauber oder Rummel) von Nutzen sein. Dabei handelt es sich um eine Server-Anwendung für PHP oder Java, die als Gadget- und Opensocial-Laufzeitumgebung fungieren kann. Getestet, gebaut und gesteuert wird Shindig mit Maven. Sind Java und Maven lokal installiert und die Shindig-Quellen aus dem Apache-Subversion-Repository ausgecheckt, erzeugt ein *mvn* das nötige Repository, bestehend aus vielerlei Bibliotheken mit ihren jeweiligen Abhängigkeiten.

mvn -Prun führt die Container-Webapplikation mit dem Applikation-Server Jetty aus. Einfache Gadget-Anwendungen enthält Shindig bereits. Sie lassen sich per http://localhost:8080/gadgets/files/container/sample1.html (bis sample7.html) ausführen. Neben diesen einfachen Applikationen kann http://localhost:8080/gadgets/files/samplecontainer/samplecontainer.html eine Laufzeitumgebung für Gadgets ausführen. Eigene Gadgets lassen sich durch Kopieren der XML-Datei in das Unterverzeichnis *$HOME/shindig/javascript/container/* installieren.

mvn package kopiert die erforderlichen Dateien nach */gadgets/target/gadgets/files/container*. Die genannte

Auf dem Weg zur Monetarisierung

Anwendungen für soziale Netze müssen keineswegs Spielerei, sondern können durchaus professionelle Unterfangen sein. Gregor Marwedel hat die Fahrplanauskunft für die Deutsche Bahn als Google-Gadget entwickelt. *iX* sprach mit dem Inhaber der nexxis Mediaconsult GmbH & Co KG.

iX: Wie sind Sie dazu gekommen, die Fahrplanauskunft der Deutschen Bahn als Google-Gadget umzusetzen?

Gregor Marwedel: Motivation bei der Erstellung des Gadget war, neben dem Ausprobieren dieser neuen Art der Nutzung die möglichst hohe Verbreitung zu testen. Wir messen das Gadget mit Google Analytics. Im Juni wurden 665 048 Seitenzugriffe bei 387 021 eindeutigen Zugriffen registriert. Zum Vergleich wurden im Zeitraum vom 25. 6. bis 25. 7. bereits 889 639 Seitenzugriffe bei 519 953 eindeutigen Zugriffen gemessen. Seit Anfang November letzten Jahres, als das DB-Fahrplanauskunfts-Gadget live ging, geht die Kurve der Aufrufe steil nach oben.

iX: Wollen Sie derartige Anwendungen auch für Facebook oder Myspace entwickeln?

G. M.: Ja, ich werde sukzessive meine Gadgets auch für alle anderen Plattformen erstellen, insbesondere natürlich Facebook und Myspace. Hierbei achte ich aber auf Affinität der Gadgets zu den Benutzergruppen beziehungsweise andersherum: Es wird Gadgets geben, die nur auf bestimmten Plattformen laufen beziehungsweise nur für diese erstellt werden.

iX: Wie lassen sich Dienste dieser Art Ihrer Meinung nach monetarisieren?

G. M.: Die Monetarisierung ist aktuell noch problematisch. Wie man es ja an Rockyou, Slide und Clearspring sehen kann, ist das Thema hochaktuell, aber momentan immer noch auf die Generierung und Steigerung von Traffic ausgelegt. Dieses muss und wird aber mittelfristig monetarisiert werden (und muss, bei den Summen, die hier immer wieder in Finanzierungsrunden oder Aufkäufe geflossen sind). Eine relativ einfache Form der Monetarisierung sind die Shopping-Gadgets, bei denen der komplette Kaufprozess im Gadget abgebildet wird – wie bei Shopit oder Radicalbuy zu finden. Monetarisierung bei Gadgets wie dem Bahn-Gadget sind da deutlich komplizierter, da das Gadget nicht auf Umsatzgenerierung ausgelegt ist. Aber natürlich könnte man beispielsweise eine Möglichkeit zum Kauf von Bahntickets oder Ähnliches implementieren und daran dann über einen Revenue Share partizipieren.

iX: Googles Gadget-API bietet die Grundlage der Opensocial-API. Gibt es Bestrebungen, die Fahrplanauskunft um weitere „soziale“ Funktionen auszudehnen?

G. M.: Beim Gadget der Fahrplanauskunft ist derzeit nicht angedacht, weitere soziale Funktionen zu integrieren. Weitere Gadgets und Projekte mit ebendiesen Komponenten sind bereits in der Planung beziehungsweise Umsetzung.

Listing 6: Nutzung von CSS innerhalb der Gadget-Definitionsdatei

```
<Content type="html">
<![CDATA[
<style type="text/css">
    #gadget {
         width: 100%;
         height: 100%;
         background-color: white;
         margin: 0px;
         padding: 0px;
    }
    /* ... */
</style>
<!-- ... -->
]]>
</Content>
```

Listing 5: Einfache Debug-Ausgabe in Javascript

```
function debug(msg) {
  if (debug) {
    debug_html += msg;
    document.getElementById("debug_div").innerHTML = debug_html;
  }
}
```



Die Anmeldung einer Opensocial-Anwendung, hier bei Orkut, ist eine Art „Bewerbung“ (Abb. 3).

samplecontainer-Datei stellt das eigene Gadget wie in Abbildung 2 dar und erlaubt, es zu testen. Ein kurzes Tutorial (im Paket enthalten) gibt darüber hinaus hilfreiche Tipps.

Debugging im Gadget-Code

Die lokal installierte Container-Umgebung bewahrt naturgemäß niemanden vor Fehlern in der eigenen Anwendung. Google beschreibt in „Gadget Development Tools [j] die Nutzung eines speziellen *div*-Elements im HTML-Bereich des Opensocial-Gadgets, das für die Ausgabe von Statusmeldungen oder der Inhalte von Variablen dienen kann. Mit

```
<div id="debug_div"
 style="font-size:9pt; padding:5px;
 color: red;">
</div>
```

wird dieses *div*-Element im Content-Bereich des Gadget angelegt und über eine Ausgabefunktion mit Inhalten beschickt.

Aussehen und Layout einer Opensocial-Anwendung kann ein Entwickler, ganz im Sinne von Webanwendungen, mit Cascading-Stylesheet-Definitionen bestimmen. Lokal lässt sich dies innerhalb des Gadget wie in Listing 6 nutzen.

Performance und Skalierung

Hat man alle bis jetzt beschriebenen Zutaten zu einer lauffähigen, lokal getesteten Opensocial-Anwendung zusammengebaut, bleibt nur noch die Veröffentlichung des eigenen Werkes. Gerade wenn man die Opensocial-Anwendung selber hosten will, gilt es, ihre Verbreitung im Vorfeld abzuschätzen.

Da einige soziale Netze über mehrere Millionen Nutzer verfügen, können je nach Attraktivität und Nützlichkeit der eigenen Anwendung schnell 200 000 Aufrufe pro Tag zusammenkommen, was etwa zwei Anfragen pro Sekunde entsprechen kann. Je nach verwendeten Daten rauschen schnell einige Hundert GByte pro Monat durch die Leitung.

Opensocial-Gadgets haben zwar von Haus aus einige Möglichkeiten zum Inhalts-Caching eingebaut, allerdings schützt dies den eigenen Server vor Überlastungen nur unzureichend. Generell sollte man gerade beim Zugriff auf externe Quellen darauf achten, wie performant dies geschieht. Dagegen ist die eigentliche Veröffentlichung eher trivial. Google mit iGoogle beziehungsweise Orkut (siehe Abbildung 3) und viele andere Mitglieder der Opensocial-Allianz bieten ihren Nutzern die Veröffentlichung von Opensocial-Anwendungen an. Naturgemäß kann ein Artikel wie dieser nicht alle Aspekte einer Opensocial-Anwendung beschreiben. Insbesondere der soziale Austausch von Daten und die Option, in Interaktion mit dem Nutzer der eigenen Anwendung zu treten, wäre Thema eines anderen Artikels. (hb)

Onlinequellen

[a] Shindig-Projekt	incubator.apache.org/shindig/
[b] Googles Gadget-XML-Referenz	code.google.com/apis/gadgets/docs/reference.html
[c] XML-Schema (XSD) von Googles Gadget-XML	opensocial-resources.googlecode.com/svn/spec/0.8/gadgets/gadgets-extended.xsd
[d] Referenz zu Opensocial 0.8	code.google.com/apis/opensocial/docs/0.8/reference/
[e] Messages Bundles	www.google.de/intl/de/apis/gadgets/i18n.html#Bundles
[f] Gadget Guidelines	www.google.com/webmasters/gadgets/guidelines.pdf
[g] Googles Gadget Editor (GGE)	code.google.com/apis/igoogle/docs/igoogledevguide.html
[h] Google Code	code.google.com/
[i] Einbindung entfernter Inhalte	code.google.com/apis/gadgets/docs/remotecontent.html
[j] Gadget Development Tools	code.google.com/apis/gadgets/docs/tools.html

RAMON WARTALA

ist IT-Leiter beim Hamburger Onlinevermarkter orangemedia.de GmbH und Koautor des bei Addison-Wesley erschienenen „Webanwendungen mit Ruby on Rails“.

Literatur

[1] Ramon Wartala; Soziale Netze; Aufgeschlossen; Was Googles Opensocial-API leistet; *iX* 7/08, S. 90





Acrobat 9
mit Flash-Integration



Noch professioneller

Thomas Merz

Mit Acrobat 9 erweitert Adobe den Einsatz der Software für Unternehmen und integriert die Flash-Mitgift von Macromedia. Wert legt der Hersteller zudem auf die Einhaltung von Standards.

Die Betonung von ISO-Standards, erweiterte Präsentationsmöglichkeiten, Verzahnung mit Onlinediensten, Verbesserungen im 3D-Bereich und die Integration von GIS-Funktionen – so könnte man die Neuerungen von Acrobat 9 zusammenfassen. Vielleicht mit Ausnahme der Flash-Integration gibt es keine spektakulären Highlights, sondern viele Funktionen, die auf diverse Aspekte des professionellen Einsatzes der Publishing-Software zielen. Äußerlich kommt die neue Version ohne große Umwälzungen aus – wohltuend für Anwender, die sich nach dem Umstieg nicht in völlig neuen Menüstrukturen verzetteln oder ein neues Benutzungsparadigma lernen wollen.

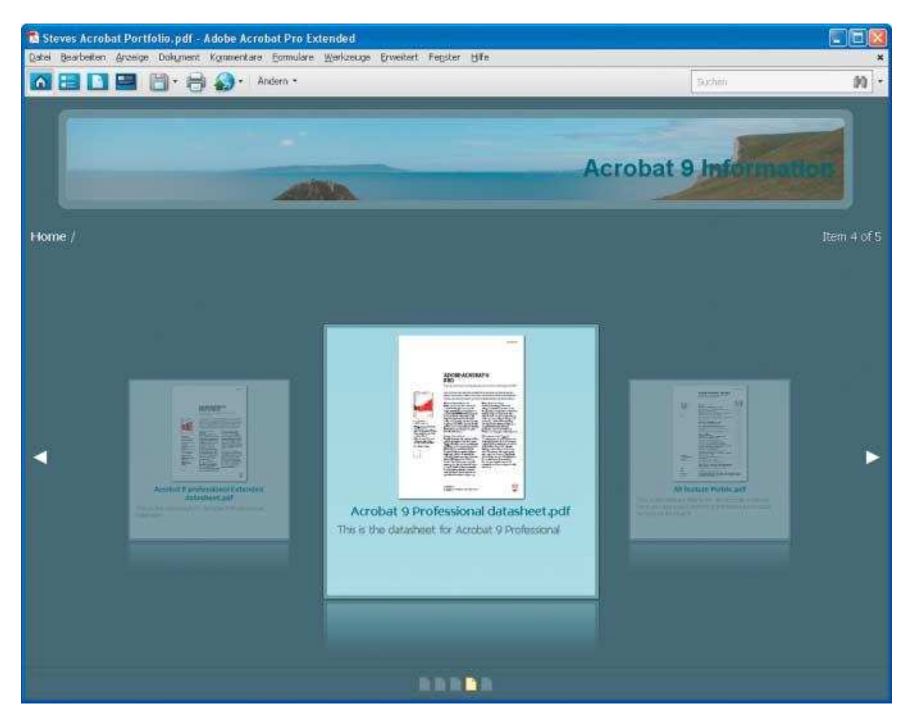
Etwas modifiziert hat Adobe die Produktstruktur: Neben der „kleinen“ Standardversion gibt es wie bisher die weiter ausgebaute Pro-Variante. Letztere enthält im Gegensatz zur Standardversion die im Folgenden näher beschriebenen Funktionen Preflight, PDF-Portfolios, Schwärzung, Reader-Aktivierung sowie einige weitere. Darüber hinaus bietet Adobe ein weiteres Paket mit der Bezeichnung Acrobat 9 Pro Extended an, das diesem Test zugrunde lag. Es umfasst zusätzlich den Livecycle Designer zur Erstellung von Formularen, das Add-on Presenter für die Umwandlung von Powerpoint-Präsentationen in animiertes PDF sowie die 3D-Funktionen, die bisher nur als separates Einzelprodukt Acrobat 8 3D erhältlich waren.

Dynamische und statische Inhalte verzahnen

Auf mehreren Ebenen hält die mit der Akquisition von Macromedia 2005 zu Adobe gewanderte Flash-Technik Einzug in Acrobat. Der Flash-Player ist sowohl in die kommerziellen Acrobat-Versionen als auch in den kostenlosen Adobe Reader integriert, was die Verzahnung statischer und dynamischer Inhalte deutlich erleichtert und das Abspielen von FLV- und H.264-Videos ermöglicht.

Flash spielt zudem eine wichtige Rolle beim neuen Onlinedienst Acrobat.com. Der ist zwar noch im Beta-Stadium und formal nicht Bestandteil des Produkts Acrobat 9, bietet jedoch bereits jetzt eine Infrastruktur für die Kollaboration auf Basis von PDF-Dokumenten. Acrobat.com, zurzeit mit einer kostenlosen Anmeldung nutzbar, bietet im Browser Funktionen zur Speicherung und gemeinsamen Nutzung von PDF-Dokumenten. Der Austausch von Kommentaren zu PDF-Dateien lässt sich darüber ebenfalls abwickeln, ohne dass der Anwender sich wie bei den bisherigen WebDAV-basierten Lösungen Gedanken über geeignete Serverkonfigurationen machen müsste. Auch ein Online-Editor namens Buzzword ist in Acrobat.com integriert. Wegen des Beta-Zustands soll hier keine Wertung des Onlinedienstes erfolgen. Es sei jedoch angemerkt, dass der in Flash implementierte Player derzeit noch keine mit Flash animierten PDFs anzeigt und bei einigen anderen PDF-Funktionen ebenfalls passen muss.

Schließlich lassen sich mit Flash-Unterstützung attraktive (manchmal auch: aufdringliche) Coverseiten für PDF-Portfolios erstellen. Dabei handelt es sich um einen neuen Namen für die bereits mit der Version 8 eingeführten Collections (PDF-Pakete). Sie fungieren als Container für mehrere PDF-Dokumente, die Acrobat innerhalb einer Datei als Gruppe zusammenfasst. Adobe nennt Angebots- und Marketingunterlagen oder umfangreiche Anmel-



PDF mit iPod-Feeling: Die Coverseiten von PDFs lassen sich mit Flash aufpeppen (Abb. 1).

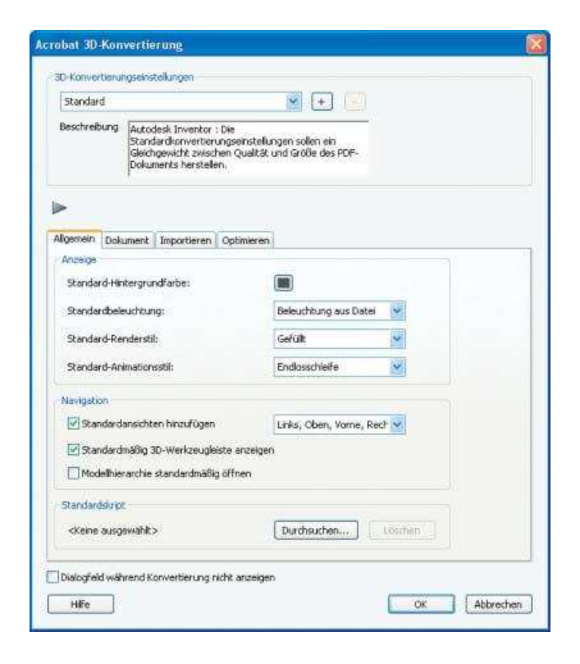
dungen in regulierten Industriezweigen, etwa der Pharmaindustrie, als typische Anwendungen. Da man die Dokumente anders als mit Acrobat 8 jetzt in einer hierarchischen Struktur anordnen darf, lassen sich selbst große Dokumentsammlungen als Portfolio zusammenfassen.

Den Rahmen dafür (vielleicht eher: die Benutzeroberfläche) stellen wiederum Flash-Animationen dar, die der Ersteller eines Portfolios anpassen kann. Wie beim Einsatz von Flash auf Webseiten deckt die Integration von Flash in PDF einen weiten Spannungsbogen von der Betonung einer Aussage durch Animation über die erleichterte Aufnahme von Informationen durch Visualisierung bis hin zu – na ja – überflüssiger Belästigung des Nutzers ab.

Verschlüsselungen sind schwerer zu knacken

Für den Schutz von PDF-Dokumenten hat der Hersteller jetzt die AES-Verschlüsselung mit 256 Bit integriert (bisher gab es in Acrobat nur 128-Bit-Schlüssel für AES). Dies klingt nach deutlich mehr Schutz vor dem „Knacken“ der Verschlüsselung, insbesondere deswegen, weil der AES-Standard statt der 10 Runden bei 128 Bit die Rundenzahl bei 256 Bit auf 14 erhöht. Immerhin hat die NSA das Verfahren AES-256 in den USA für die Verschlüsselung von Dokumenten der Klasse „Top Secret“ zugelassen. Bei alldem sollte man jedoch nicht vergessen, dass der Key aus einem Passwort generiert wird, das in PDF auf 32 Zeichen Länge begrenzt ist, was den Schlüsselraum gehörig einschränkt. Schlechte Passwörter lassen sich auch durch lange Schlüssel nicht kompensieren.

Eine weitere Facette des Themas Sicherheit steckt hinter der Schwärzungsfunktion, die Adobe schon mit Acrobat 8 eingeführt, in der neuen Version jedoch noch einmal aufgewertet hat. So kann der Anwender jetzt alle Vorkommen eines Begriffs automatisch und sicher schwärzen lassen. Dabei wird der Text nicht einfach mit einem Balken „überklebt“, sondern rückstandsfrei aus dem Dokument entfernt. Dass es Bedarf für eine solche Funktion gibt, zeigen etliche Vorkommnisse aus den letzten Jahren, bei denen vertrauliche Informationen wegen unzureichender Schwärzung von PDF durch einfaches Überkleben ungewollt an die Öffentlichkeit gelangten. Selbst mit den integrierten Werkzeugen von Acrobat konnte ein einigermaßen versierter Anwender bisher die Schwärzung entfernen und den vertraulichen Text wieder zum Vorschein bringen.



Acrobat 9 Pro Extended konvertiert 3D-Modelle auch ohne die zugehörige Originalanwendung (Abb. 2).

Das PDF-Dateiformat selbst ist mittlerweile so ausgereift, dass keine großen Erweiterungen erforderlich waren. Die Stabilisierung von PDF zeigt sich auch in der Tatsache, dass das Format vor einigen Monaten unter der Bezeichnung ISO 32000 zum internationalen Standard geadelt wurde. Die wenigen Erweiterungen, die Adobe seit Beginn des Standardisierungsprozesses für PDF 1.7 hinzufügte und in Acrobat 9 implementierte, erscheinen in der Datei als nummerierte Extensions – ganz so, wie es ISO 32000 vorschreibt. Acrobat 9 führt also keine neue PDF-Version mit eigener Versionsnummer ein, sondern erzeugt PDF 1.7 mit kleineren Erweiterungen.

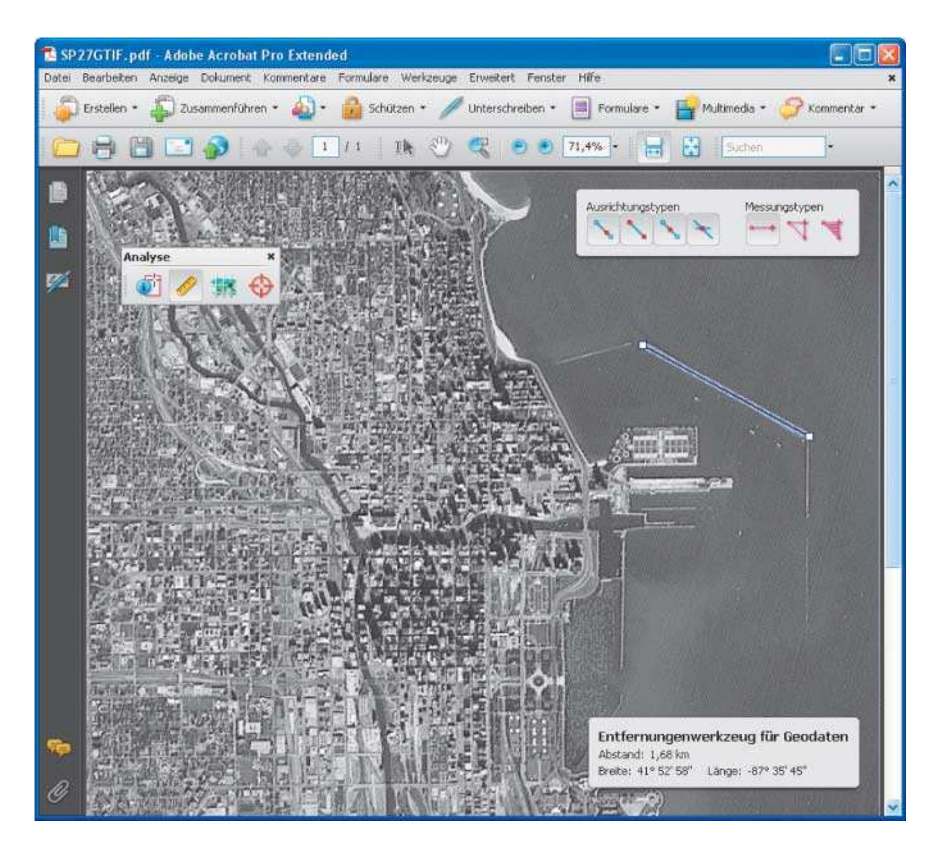
Strenge Einhaltung der ISO-Standards

ISO-Standards spielen in der neuen Version generell eine wichtige Rolle: Ein eigenes Standards-Panel klärt den Anwender darüber auf, ob ein Dokument den Vorgaben von PDF/A für die Archivierung, PDF/X für die Druckvorstufe oder PDF/E für den Engineering-Bereich entspricht. Bei diesen ISO-Standards handelt es sich um Teilmengen von ISO 32000 für bestimmte Anwendungsbereiche. Die Einhaltung dieser Standards überprüft das aktualisierte Preflight-Plug-in, das wie schon bei den Vorgängerversionen wieder die Berliner Firma Callas Software beigesteuert hat. Die Entwickler haben nicht nur die Benut-

zung von Preflight vereinfacht, sondern zusätzlich striktere Prüfungen implementiert mit der Folge, dass das Plug-in jetzt auch subtile Standardverletzungen erkennt. Das bedeutet aber gleichzeitig, dass etliche PDFs, die bisher noch als standardkonform galten, in Acrobat 9 Fehlermeldungen bei der Validierung liefern. Dies zwingt wiederum die Hersteller von PDF-Erstellungssoftware an die Tastatur, um die von Acrobat 9 aufgedeckten Unzulänglichkeiten in ihrer PDF-Ausgabe zu beheben.

Ersteller und Anwender von Geodaten können sich darüber freuen, dass PDF-Dokumente jetzt georeferenzierte Karten enthalten können. Beim Import von GeoTIFF- oder JPEG2000-Bildern mit Referenzinformationen werden diese übernommen und es wird daraus georeferenziertes PDF erstellt. Die so entstandene Beziehung zwischen PDF und „richtiger Welt“ lässt sich nutzen, um etwa für einen Punkt auf der Karte dessen Längen- und Breitengrad anzuzeigen oder umgekehrt die Position auf der Seite hervorzuheben, die einem bestimmten Koordinatenpaar entspricht. Software für den Umgang mit georeferenziertem PDF gab es bisher schon vom US-Hersteller Terrago als proprietäres Plug-in für Acrobat 6 und höher. Ob der Hersteller das Produkt trotz der umfangreicheren Funktionen gegen die Übermacht von Adobe halten kann, muss sich zeigen.

Für vorhandenes Kartenmaterial kann der Anwender die Referenzdaten zwar manuell eingeben, richtig komfortabel wird diese Funktion allerdings erst, wenn die GIS-Software dies gleich beim Exportieren von PDF unterstützt. Als erster GIS-Hersteller hat ESRI als Ergebnis einer Kooperation mit Adobe angekündigt, georeferenziertes PDF zu exportieren. Speichert der Anwender solche PDFs mit der Acrobat-Vollversion als „Reader-aktiviert“, stehen die erweiterten Geo-Funktionen im Adobe Reader ebenfalls zur Verfügung. Dieses Verfahren gab es bisher schon, um Benutzern des Adobe Reader das Speichern ausgefüllter Formulare, Signieren und Kommentieren von Dokumenten et cetera zu erlauben. Da diese Aktivierung auf einer digitalen Signatur basiert, lässt sie sich nur mit Adobe-Software, nicht aber mit Produkten von Drittherstellern durchführen.



In georeferenzierten PDF-Bildern lassen sich Längen- und Breitengrad anzeigen sowie reale Strecken und Flächen messen (Abb. 3).

Acrobat 9 für Windows steht in allen drei Varianten ab sofort zur Verfügung. Für Mac OS X hat Adobe nur die Pro-Version im Programm (der frei verfügbare Reader ist in der neuen Version auch schon für Mac OS verfügbar, allerdings noch nicht für alle unterstützten Plattformen). Vergünstigte Upgrades bietet der Hersteller für vorhandene Lizenzen von Acrobat 6 oder höher an. (ka)

THOMAS MERZ

ist Geschäftsführer der PDFlib GmbH in München, die serverbasierte PDF-Werkzeuge entwickelt. Er ist außerdem Leiter der Technical Working Group des PDF/A Competence Center.

Daten und Preise

Acrobat 9

Hersteller: Adobe Systems, www.adobe.de

Softwarevoraussetzungen: Windows XP oder höher, Mac OS X 10.4.11 oder 10.5

Hardwarevoraussetzungen: 512 MByte RAM

Preise: Standard: 349 € (Upgrade: 115 €), Pro: 559 € (Upgrade: 189 €), Pro Extended: 819 € (Upgrade: 269 €)

iX-Wertung

⊕ Ausbau der Funktionen für den professionellen Einsatz

⊕ Betonung von Standards

⊕ verbessertes Preflight-Plug-in

⊕ Flash-Integration

⊕ georeferenzierte Dokumente



Google Web Toolkit 1.5 auf Basis von Java 5

Mit Köfferchen

Michael Seemann

Rich Web-Clients mit Ajax zu entwickeln erfordert ein unterstützendes Framework auf Client- oder Serverseite. Googles zwei Jahre altes Web Toolkit, das in Java implementiert ist, kommt jetzt in der Version 1.5.

Ende Mai dieses Jahres hat Google die erste Vorab-Release ihrer Web-Toolkit-Version 1.5 veröffentlicht, im Juli lag der Release Candidate 1 vor. Geht man von einem ähnlichen Entwicklungsverlauf wie bei der Version 1.4 aus, sollte das Modell 1.5 Anfang September zum Download verfügbar sein. Besonders für Webentwickler, die Java als Entwicklungssprache benutzen, ein wichtiges Ereignis.

Zwei Jahre nach Veröffentlichung des Web Toolkit (siehe [1]) kann man wohl mit Recht behaupten, dass der Weg, den Google mit ihm beschritten hat, richtungsweisend war. Das Toolkit hat die effektive Entwicklung von Ajax-Anwendungen ermöglicht. Gerade in einem Umfeld, in dem die Implementierung auf dem Server in Java erfolgt, ist der Einsatz des GWT eine vernünftige Lösung. Man kann auf diese Weise nicht nur den Servercode in Java implementieren, sondern außerdem den Client. Das GWT sorgt für die Übersetzung des Java-Quellcodes nach Javascript, und der Browser kann die Anwendung starten. Besondere Anforderungen stellt das Toolkit an den Client nicht; es genügt ein aktueller Webbrowser mit aktiviertem Javascript.

Ein Manko hatte die bisherige Version – sie konnte nur Java-Quellcode übersetzen, der zu Java 1.4 konform war. Hatte man schon die Umstellung auf eine neuere Java-Version vollzogen und beispielsweise Generics im Code verwendet, konnte das GWT mit ihm nichts anfangen. Version 1.5 soll diese Hürde überwinden und die Sprachmittel von Java 5 unterstützen. Neben den Generics handelt es sich vor allem um Annotations und typsichere Aufzählungen (*enum*). Die nächste Version bringt darüber hinaus an der Oberfläche einiges an Neuem.

Standard-HTML und Standard-Thema

Bei früheren Versionen des Google Web Toolkit sahen die Widgets eher spartanisch aus. Vor allem, wenn diese nicht auf Standard HTML-Elementen basierten, hat man ohne angepasste Stylesheets in der Regel nicht viel auf der Oberfläche gesehen. Gerade diese ersten Schritte vereinfacht das GWT nun mit Oberflächen-Themes, die sich in der Modulkonfiguration aktivieren lassen. Die Abbildung zeigt das Standard-Theme, das GWT beim Erstellen des Grundgerüstes einer Anwendung mit dem *applicationCreator*-Skript aktiviert. Keine Angst, niemand ist daran gebunden, ein bestimmtes Theme zu verwenden – man kann selbst für das Erscheinungsbild der Anwendung sorgen.

Erfreulich, dass die neue Version den Standard-Modus der Webbrowser komplett unterstützt. Das war in den Vorgängerversionen anders – die kamen mit dem Quirks-Modus besser zurecht – ein Stolperstein für Entwickler, die sich an Standards orientierten.

Eine Runderneuerung hat auch die Unterstützung verschiedener Landessprachen erfahren. Selbst mit von rechts nach links gelesenen Sprachen kann das GWT umgehen. Dabei verhalten sich die Widgets zur Anordnung von Oberflächenelementen konform zur Leserichtung. Neu ist außerdem, dass der Entwickler Pluralformen seiner Ressourcedateien erstellen kann. Die Konfiguration erfolgt über einen Satz von Annotations. Den Rest erledigt das GWT. Grammatikalische Unfälle der Form „Sie haben 2 neues Auto“ sollten damit der Vergangenheit angehören. Ebenfalls erfreulich ist die Unterstützung von ARIA (Accessible Rich Internet Applications (siehe [b]) bei vielen Oberflächenkomponenten.

Wer kein Freund abrupter Übergänge ist, dürfte seine Freude an den neuen Animationsfähigkeiten des GWT haben. Trees klappen sanft auf, Pop-ups werden beim Anzeigen vergrößert und schrumpfen beim Ausblenden zusammen. Die Reiter der *TabPane* werden ein- und ausgeblendet, um einige Beispiele zu nennen. Ein Aufruf von *setAnimationEnabled(true)* aktiviert diese Fähigkeit.

Google hat das Zusammenspiel von Javascript- und Java-Objekten verbessert. Anstelle der durchgehenden Verwendung einer einfachen Referenz auf Javascript-Objekte kann man nun Java-Klassen schreiben, die von der Klasse *JavaScriptObject* erben. Dadurch lassen sich Javascript-Bibliotheken deutlich

iX-Wertung

⊕ Der GWT-Compiler unterstützt die Java 5 Syntax.

⊕ Standard-Themes erleichtern den Einstieg.

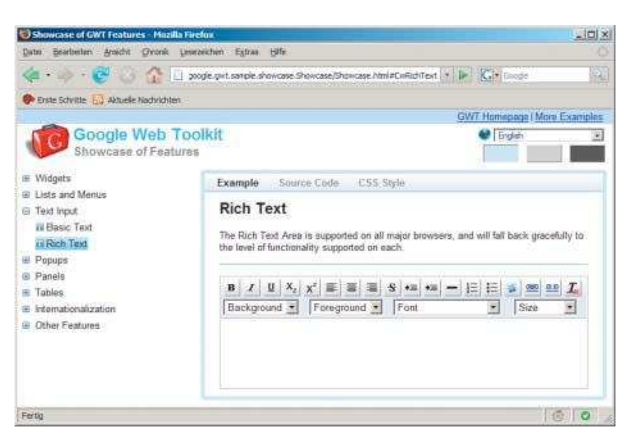
⊖ komplexe Regeln für die Einbettung von Javascript

besser in die GWT-Welt integrieren. Statt Wrappern können Programmierer die Objekte solcher Bibliotheken direkt durch eine GWT-Klasse modellieren. Der Zugriff auf die Eigenschaften ist weiterhin über das Javascript Native Interface erforderlich – allerdings hat man Zugriff auf den *this*-Zeiger der Javascript-Objekte. Die Restriktionen für solche Klassen sind nicht unerheblich: So müssen beispielsweise alle Instanz-Methoden als *final* deklariert sein. Deshalb kann man zu einer Klasse nur Methoden hinzufügen, sie aber nicht verbergen oder gar überschreiben.

Wer hier nicht in Fallen tappen möchte, tut gut daran, die Sprachmittel von Java zu benutzen und schon beim Design der Klassen für die Einhaltung dieser Bedingung zu sorgen. An solchen Stellen zeigt sich ein immenser Vorteil des GWT-Weges: Man kann Regeln auf Sprachebene definieren, die ein Compiler prüfen kann. Das gilt generell. So kann Javascript beispielsweise nicht eine Schnittstelle definieren und Klassen zur Implementierung dieser Schnittstellen zwingen – Java schon.

Das sind aber noch nicht alle Verbesserungen, die unter der Haube stattgefunden haben. Die für den Datenaustausch zwischen Client und Server vorgesehenen Klassen müssen nun nicht mehr über einen öffentlichen Konstruktor verfügen, was ein besseres Klassendesign erlaubt. Ebenso wichtig für das Thema Serialisierung ist die Unterstützung von Klassen aus dem *java.sql*-Package. In früheren Tagen war es eine häufige Fehlerquelle, wenn der Server ein Datum über eine JDBC-Schnittstelle aus der Datenbank holte und plötzlich anstelle eines *java.util.Date* ein *java.sql.Date* zum Client übertragen sollte – mit dem Ergebnis einer Runtime-Exception. Nicht mehr nötig ist eine spezielle Ausnahme, die von der Klasse *SerializableException* ableitet, da die Klasse *Throwable* nun serialisierbar ist.

Fortschritte sind ebenso bei der Emulation des Java Runtime Environment zu verzeichnen. Die Methoden *Object.getClass()* und *Class.getName()* lassen sich nun verwenden, was das Aus für die Hilfskonstruktion *GWT.getTypeName()* bedeutet. Freunde von typisierten Arrays dürften sich über die Unterstützung von *Arrays.asList()* freuen, da man so leicht an die Vorteile der Collection-API kommt und beispielsweise die *contains*-Methode verwenden kann.



Demo im Standard-Oberflächen-Theme: Ein Rich-Text-Editor stellt je nach Plattform die unterstützten Eigenschaften im Menü dar.

Umsteigen auf die neue Version

Für den Umstieg auf die neue GWT-Version muss die Laufzeit- und Entwicklungsumgebung (etwa Eclipse) mindestens mit Java 5 laufen. Anschließend lädt man das GWT 1.5 herunter und ersetzt die Java-Archive *gwt-dev-windows.jar* (oder das passende Gegenstück, für das verwendete Betriebssystem) und *gwt-user.jar* in der Entwicklungsumgebung. Die GWT-Shell ist nun startklar, und die unter GWT 1.4 entwickelte Anwendung läuft unter GWT 1.5. Idealerweise hatte man schon ein Build-Script verwendet. In solchem Fall muss man nur das GWT-Home-Verzeichnis anpassen. Tauscht man außerdem auf dem Server die Datei *gwt-servlet.jar* aus, ist der Umstieg abgeschlossen und man profitiert umgehend von den Laufzeit-Optimierungen.

Soweit die Theorie. In der Praxis ist die Vorabversion leider noch nicht ganz frei von Fehlern (erwartungsgemäß). Beim Versuch, das Fitnesstagebuch des Autors [c] auf Version 1.5 umzustellen, offenbarte der Compiler noch ein paar Schwierigkeiten bei der Übersetzung der RPC-Klassen, die eine Initialisierung in einem privaten Konstruktor durchführten. Ein Workaround, der auf eine vollständige statische Initialisierung umstellte, konnte den Stolperstein aber beseitigen.

Wie zu erwarten ist damit der Umstieg nicht abgeschlossen. Man muss alle als „lieber nicht mehr zu verwenden“ (engl.: „deprecated“) markierten Klassen und Methoden anpassen. Dazu zählt die Klasse *HTTPRequest*, die man durch die Klasse *RequestBuilder* ersetzen muss. Andernfalls steht man bei der nächsten Version vor einem riesigen Berg voll Arbeit, und der Umstieg ist nicht so einfach wie oben beschrieben.

Zur Code-Umstellung gehört, dass man die Klassen der Collection-API (*HashMap*, *List* et cetera) parametrisiert benutzt. Die Entwickler des GWT haben unter anderem daran gedacht, das Interface *AsyncCallback* zu parametrisieren. Damit können Programmierer auf umständliche *casts* in der Methode *onSuccess* verzichten und so das Laufzeitverhalten stabilisieren.

Fazit

Ein Umstieg auf GWT 1.5 lohnt sich. Nur wer an Java 1.4 gebunden ist, sollte Abstand davon nehmen. Neben den Verbesserungen im Compiler, der effizienteren Javascript-Code generiert, spricht die Unterstützung von Java 5 für den Umstieg. Sogar ohne die Sprachmöglichkeiten von Java 5 verfügt man über Verbesserungen, die sich nicht nur an der Oberfläche zeigen, sondern die Programmierung von GWT-Anwendungen und die Integration von Javascript-APIs erleichtern. (hb)

MICHAEL SEEMANN

ist Diplom-Wirtschaftsinformatiker. Er arbeitet als selbstständiger Softwareentwickler, Berater und Fachautor.

Onlinequellen

[a] Google Web Toolkit	code.google.com/webtoolkit/
[b] ARIA: Accessible Rich Internet Applications	developer.mozilla.org/en/docs/Accessible_DHTML
[c] Fitnesstagebuch	www.gwt-buch.de/fitnesstagebuch

Literatur

[1] Christoph Leisegang, Stefan Mintert, Bastian Spanneberg; Web 2.0; Die Nullnummern; Fünf serverseitige Ajax-Frameworks; *iX* 9/2006, S. 66







Parallels' Server auf dem Mac

Auf dem Sprung

Jörg Riether

Virtualisierungsspezialist Parallels, vor allem bekannt durch die etablierten Produkte Desktop (Mac) und Workstation (Windows und Linux), hat seinen jüngsten Spross veröffentlicht, den Parallels Server 3.0 für Mac.

Parallels' Server sei die weltweit erste Server-Virtualisierungslösung für die Mac-Plattform, so der Hersteller plakativ auf seiner Homepage. Und in der Tat hat sich einiges getan. Der neue Server, der übrigens die Versionsnummer 3.0 trägt, obwohl es sich um die erste veröffentlichte Inkarnation handelt, kommt gleich in großer Vielfalt daher. Neben der Mac-Version mit Produktivstatus gibt es drei in der Entwicklung befindliche Versionen, die zum Redaktionsschluss noch Betastatus hatten: den Parallels Server für Windows, für Linux und eine echte Bare-Metal-Variante. Sie läuft ähnlich wie VMwares ESX aus einem Guss als eigenständiger Hypervisor auf der Hardware.

Verglichen mit dem Desktop-Produkt für Mac hat der Hersteller an einigen Schrauben gehörig gedreht. Gleich eingangs sei erwähnt, dass er die Gastunterstützung speziell für die Anforderungen speicher- und performancehungriger Systeme erheblich verbessert hat. So bietet Parallels' Server pro Gast bis zu vier virtuelle Prozessoren, maximal 8 GByte Speicher und bis zu 10 virtuelle Netzwerkkarten. Darüber hinaus unterstützt er nunmehr endlich 64-Bit-Gäste – eine Funktion, auf die Parallels-Fans schon sehr lange warten. Virtuelle Festplatten dürfen bis zu 2 TByte groß sein.

Parallels Server für Mac kann laut Hersteller auf Mac OS X Server Leopard/Tiger seinen Dienst verrichten – und überraschenderweise auch auf den Desktop-Varianten. Die unterstützten Betriebssysteme umfassen die gängigen Windows-Ausprägungen 2000; XP, 2003 Server Vista und Server 2008, im Linux-Bereich finden sich Ubuntu, Suse, Red Hat, FreeBSD und Debian. Als große Besonderheit und Schmankerl virtualisiert Parallels Server für Mac auch Leopard-Server (siehe Aufmacher).

Verwaltung per Managementkonsole

Die Installation geht unspektakulär und schnell vonstatten, ein etwaiger bereits vorhandener Parallels Desktop kann nicht mit dem Parallels Server koexistieren. Diesen Sonderfall fängt der Installer sauber ab, und eine entsprechende Deinstallationsroutine startet automatisch, bevor die eigentliche Server-Installation weitergeht. Ist die Software eingerichtet, gibt es nicht wie vom Parallels Desktop gewohnt ein Interface für fast alles, sondern der Server läuft bereits als Dienst, den man mit einer Managementkonsole bedient.

Diese wirkt aufgeräumt und ist intuitiv zu bedienen (siehe Abb. 1). Wahlweise führt ein Assistent durch die Gastkonfiguration, man kann jedoch auch sämtliche Einstellungen vorab oder später manuell anpassen. Die Übersicht gliedert sich in die drei Reiter Summary, Console und Performance. Der zweite zeigt die interaktive Live-Konsole und der dritte Performance-Daten in Echtzeit. Summary und Performance sind auch zusammengefasst für den ganzen Host verfügbar und illustrieren so die globale Auslastung des Systems.

Der Assistent für die Gastinstallation fragt unspektakulär das Betriebssystem sowie die Version ab, und drei Mausklicks später steht ohne manuelle Anpassungen die virtuelle Maschine bereit. Als Besonderheit sei erwähnt, dass es Parallels' Server anscheinend egal ist, ob man einen 32- oder 64-Bit-Gast installieren möchte. Danach fragt er nämlich nicht, und er weiß ergo zur Bootzeit noch nicht, ob eine 64-Bit-Variante im (physischen oder virtuellen) optischen Laufwerk liegt. Im Test erkannte er eine DVD mit Windows Server Enterprise 2008 x64 ohne Weiteres, und das Betriebssystem ließ sich ohne Murren aufspielen.

Virtuelle Festplatten können eine feste Größe besitzen oder nach Bedarf wachsen, es besteht die Wahl zwischen virtuellem IDE oder SCSI. Sonstige Standardeigenschaften wie Shared Folders, Scripting, ein Offline-Explorer, eine virtuelle Floppy, eine Soundkarte, serieller und paralleler Port sowie vir-

tuelle optische Laufwerke sind heute selbstverständlich und fehlen auch in Parallels Server für Mac nicht. Unterstützung für USB soll in Release 3.01 folgen, ebenso für PCI VT-d, also die Zuordnung von PCI-Devices zu einer virtuellen Maschine. Zur Integration von Firewire sagt der Hersteller bislang nichts.

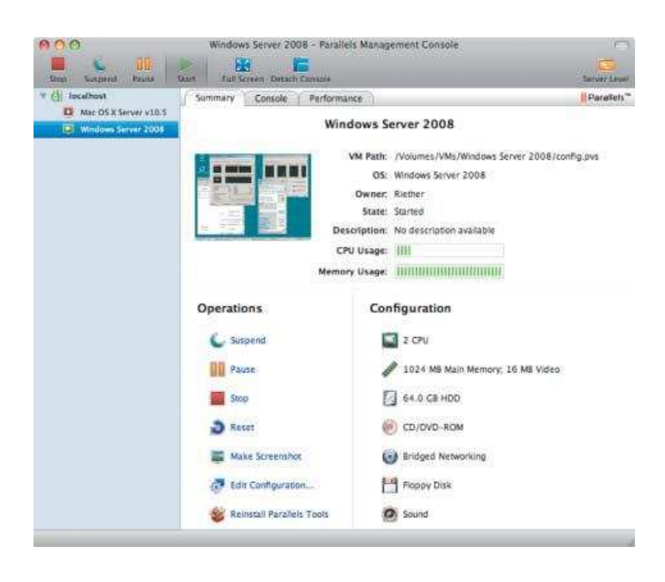
Darüber hinaus gibt es speziell auf einen Virtualisierungsserver zugeschnittene Features. Hierzu zählen ein Schalter zur Performance-Optimierung, der die Priorität dem Host oder den virtuellen Gästen gibt. Außerdem kann man den Benutzer definieren, unter dem der Gast laufen soll, und ein automatisches Verhalten beim Start (Neutral, Start, Wiederherstellung) und Shutdown (Stop, Suspend und Shutdown) des Host festlegen.

Angemessene Geschwindigkeit

Heutzutage erwarten verwöhnte Nutzer von Server-Virtualisierung eine adäquate Geschwindigkeit, vor allem im Netz. Hier erfreute der Parallels Server beim Kurztest einer simplen Übertragung einer 4 GByte großen Datei von Windows 2008 zu Windows 2008 mit anständigen Werten von 50 MByte/s. Damit nicht ein langsames System die Übertragung bremst, kam als Host ein Mac Pro mit 16 GByte RAM zum Einsatz und die virtuelle Platte fester Größe lag auf einer Raptor von Western Digital.

Wie eingangs beschrieben, unterstützt Parallels' Server auch die Servervariante von Leopard. Die Desktop-Version ließ sich jedoch nicht installieren; das Programm erkennt sie bereits während der ersten Boot-Sekunden und bricht mit einer Fehlermeldung ab. Technisch gesehen sollte der Betrieb des Mac-Desktop möglich sein. Nachfragen im englischen Forum und bei der deutschen Marketingagentur von Parallels ergaben, dass Apple in diesem Punkt ein Veto eingelegt habe. Daher dürfe die Firma zurzeit nur Leopard-Server virtualisieren.

Wenn es zum Thema Snapshots kommt, ein heute elementarer Bestandteil jeder professionellen Virtualisierungslösung, muss Parallels' Server passen: Die aktuelle Version bietet diese Funktion nicht. Wer trotzdem eine Art Lebensversicherung für einen wichtigen Test oder Patch benötigt, kann zwar virtuelle Maschinen klonen,



Vorbildlich aufgeräumt samt Livebild präsentiert sich die Übersicht der Managementkonsole des Parallels Server für Mac (Abb. 1).

aber an den Komfort eines Snapshot geschweige denn eines Snapshot-Managers kommt dies nicht heran. Da Parallels Desktop für Mac so einen Manager enthält, verwundert sein Fehlen beim Server. In Version 3.01 sollen Snapshots möglich sein; sie ist für „Ende des Sommers“ angekündigt.

Überaus merkwürdig mutet die Preisgestaltung des Produkts an. Selektiert man im Shop Euro, kostet das Produkt netto samt einem Jahr Platinum Support und Maintenance 1080 Euro. Wenn man allerdings US-$ wählt, fallen 1250 an – ebenfalls mit Wartung für ein Jahr und ohne Steuern. Beim aktuellen Kurs bekäme man rund 1700 US-$ für den geforderten Euro-Betrag. Diese Diskrepanz ist durch nichts zu begründen. Gleichzeitig demonstriert sie eine Unart, die sich seit Längerem breit macht: Immer häufiger rechnen Hersteller US-$ nahezu 1:1 in Euro um.

Fazit

Für die erste Version eines Server-Virtualisierers zeigt sich Parallels' Produkt robust und performant. Es lässt sich schnell und intuitiv bedienen und zeigte während der Tests keine nennenswerten Fehler. Im Unternehmenseinsatz sind heute jedoch Features wie Snapshots und die damit verbundenen Backup- und Testmöglichkeiten sowie Hochverfügbarkeit das A und O. Hinzu kommt eine Preisgestaltung, die in Zeiten von VMwares Server, Microsofts Hyper-V und Citrix' Xen Server Express möglicherweise nicht die gewünschten Verkaufszahlen bringt. Um sich mit seit Jahren etablierten Enterprise-Produkten wie VMware ESX Server messen zu können, fehlt noch eine Menge. Reizvoll könnte der Parallels Server für Unternehmen sein, die Mac OS X Server in hohen Stückzahlen verwenden. Hier lohnt sich ein Einsatz schon aus Energie-, Platz-, Administrations- und Wartungsgründen allemal. (ck)

JÖRG RIETHER

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisierung. Er arbeitet als Abteilungsleiter der EDV bei der Zentrum für Soziale Psychiatrie Haina gGmbH.

iX-Wertung

- ⊕ performant
- ⊕ Unterstützung für 64-Bit-Gäste
- ⊕ Virtualisierung von Mac OS X Server
- ⊖ keine Snapshots möglich
- ⊖ Preisgestaltung

Daten und Preise

Parallels Server for Mac 3.0

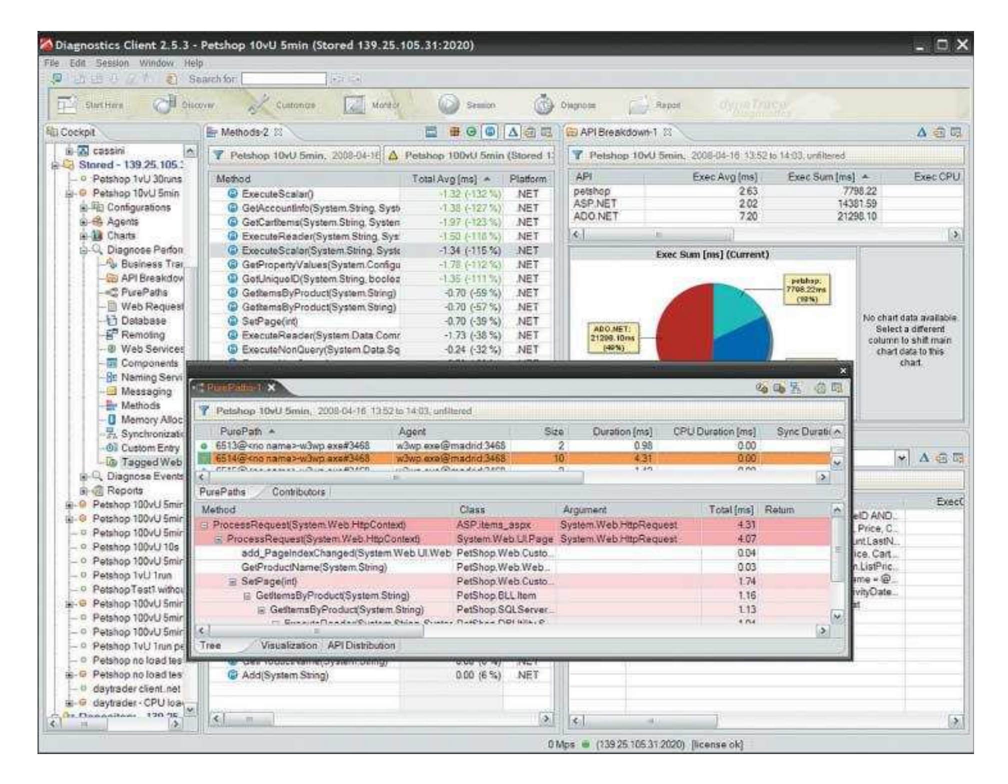
Hersteller: Parallels, www.parallels.com

Preis: 1080 Euro netto

Hardwareanforderung: Intel-Mac, 2 GByte RAM, optisches Laufwerk, 15 GByte pro VM, Ethernet- oder Firewire-Netzwerkadapter

Softwareanforderung: Mac OS X 10.5.2 oder 10.4.11, Desktop oder Server

unterstützte Gäste: Debian 3.1/4.0, FreeBSD 6/7, Red Hat Enterprise Linux 3, 4 und 5, Suse Linux Enterprise Server 9/10, Ubuntu 7.10; Windows Server 2003/2008, Vista, XP, 2000; Mac OS X Server 10.5



Dynatrace Diagnostics: Performance-Management und Fehlerdiagnose vereint

Der Pfadfinder

Frank Rometsch, Horst Sauer

Linux oder Windows, Java oder .Net, Open-Source- oder kommerzieller Applikations- und Datenbankserver – bei heutigen Geschäftsanwendungen ist nahezu alles vertreten. Das erschwert die Test- und Diagnostizierbarkeit solcher Systeme erheblich. Dem will Dynatrace mit Diagnostics begegnen.

Betraut mit der Aufgabe, die Performance und Stabilität einer unternehmenskritischen verteilten Multi-Tier-Applikation sicherzustellen, muss man einerseits den Nachweis über die Einhaltung von Service Level Agreements (SLAs) erbringen, andererseits bei einer Störung schnell reagieren, um die Ursachen zu finden und die Fehler zu beheben. Meist spielt sich das auf einer heterogenen Server-Farm ab, deren Architektur und Dynamik kaum jemand bis auf die Applikationsebene hinauf kennt. Hinzu kommt, dass sich die Rekonstruktion des Fehlers in den Entwicklungsabteilungen oft als schwierig erweist und meist mehrere Teams mithelfen müssen, was zu unnötig langen Bearbeitungszeiten führt.

Das im Jahr 2005 in Linz gegründete Unternehmen Dynatrace verspricht, mit Diagnostics sowohl das Performance Monitoring im 24 × 7-Betrieb als auch Fehlerdiagnosen durchführen zu können und den gesamten Zyklus erheblich zu beschleunigen. Den Kern und das Alleinstellungsmerkmal des Werkzeugs bildet Purepath, eine Technik, mit der der Diagnostiker Business-Transaktionen über Server-, Applikations-, Netz- und Betriebssystemgrenzen hinweg ohne Performance-Einbußen protokollieren und wenn nötig bis auf Code-Ebene hinunter verfolgen kann. Die Frage, wie weit das geht, zu beantworten ist Gegenstand einiger Praxistests mit der Version 2.6.0.

Agenten für Clienten mit eigenem Server

Dreh- und Angelpunkt bilden die sogenannten „Diagnostics Agents“, die auf den zu beobachtenden Systemen installiert sein müssen und dort nach der Platzierung der sogenannten „Knowledge Sensors“ in der Applikation deren Rohmessdaten erfassen. Der „Diagnostics Server“ sammelt die Daten aller Agenten, bereitet sie auf und stellt Berechnungen an. Die „Diagnostics Clients“ schließlich bieten eine grafische Oberfläche, auf der die Konfiguration aller Dynatrace-Komponenten und die Visualisierung der Messdaten erfolgen. Agenten, Server und Clients kommunizieren über einen konfigurierbaren TCP/IP-Port, was ein flexibles Deployment und einen verteilten Betrieb auch über das Internet erlaubt. Zusätzlich ist ein Repository für die persistente Speicherung von Messdaten im Lieferumfang enthalten. Alle Komponenten gibt es als Version für Windows und Linux, den Server außerdem für Solaris.

Diagnostics lernt Anwendungsverhalten

Erfreulich einfach geht das Installieren von der Hand, denn für alle Komponenten liegen Installationsroutinen vor. Im Falle der Agenten richten die Prozesse auf den zu beobachtenden Systemen eine einzige *.dll* bei Windows beziehungsweise eine *.so*-Datei bei Unix oder Linux ein. Über die Profiler- oder Tool-Schnittstellen der virtuellen Maschine – JVM für Java, CLR für .Net – klinken sich die Agenten mit ihren Sensoren in die jeweilige Laufzeitumgebung ein und erhalten fortan Informationen über alle relevanten Ereignisse der unter der VM laufenden Applikationen sowie über den internen Status der VM selbst (Abbildung 1).

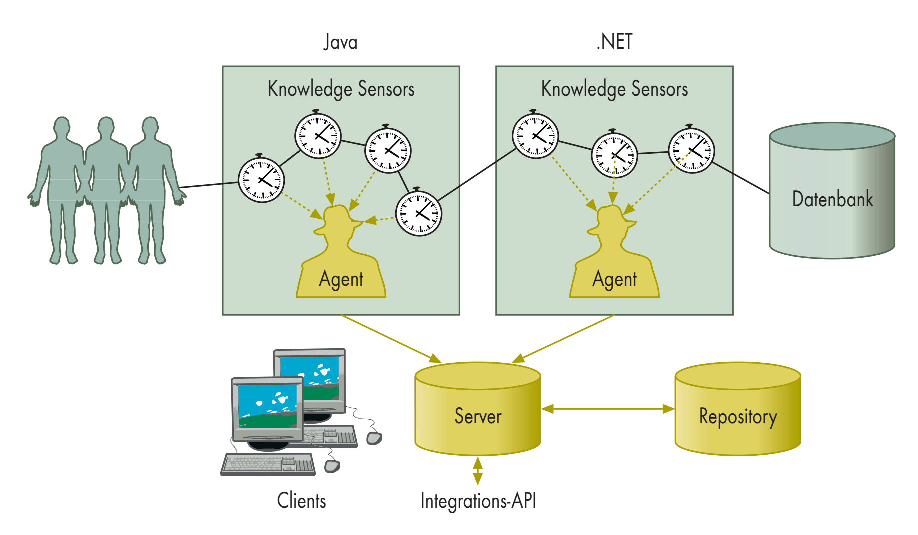
Der Systemingenieur verbindet jeden Agenten, identifiziert über einen

eindeutigen Namen, mit einem Diagnostics Server, an den er die Messdaten liefern soll. Dem ersten Start der Applikation unter „Beobachtung“ von Dynatrace, dem „Discovery Run“, kommt besondere Bedeutung zu: Beim ersten Durchgang „lernt“ Diagnostics die Klassenstruktur und weitere Metainformationen on the fly. Deshalb reagiert die Applikation anfangs schwerfälliger als vorher. Um spätere Messungen nicht durch den Lernvorgang zu verfälschen, sollte man dafür sorgen, dass der Discovery Run möglichst viele Anwendungsfälle und damit die meisten Ausführungspfade durchläuft.

Jetzt kann der Verantwortliche konfigurieren, welche Methoden er beobachten will. Beim „Sensor Placement“ sucht der Agent die ausgewählten Methoden gezielt aus. Dazu fügt er nach Bedarf Instrumentierungs-Code ein, um für jeden Aufruf Daten wie Laufzeit, CPU-Verbrauch, Kontext-Informationen, Methoden-Argumente, Aufrufer oder Exceptions zu protokollieren.

Den dadurch entstehenden Performanceverlust beziffert Dynatrace mit 3 bis 5 %; er kann aber in der Praxis erheblich darüberliegen, denn er hängt von der Laufzeit einzelner Methoden und deren Aufrufhäufigkeit ab. Kurze Methoden, die zu unverhältnismäßigem Instrumentierungs-Overhead führen würden, kann man per Konfiguration ausschließen, für Getter- und Setter-Methoden gibt es sogar eine eigene Option. Damit lassen sich die Einbußen in der Regel auf ein erträgliches Maß reduzieren.

Mit der im Produkt enthaltenen Technik Purepath kann der Analytiker einen frei wählbaren Einstiegspunkt, etwa einen Webservice oder einen normalen Methodenaufruf nebst Trace-Punkten als Sensoren im Gesamtsystem definieren. Purepath erfasst Transaktionen vom Einstiegspunkt durch alle betroffenen Schichten hindurch (siehe Abbildung 2 und Aufmacher).



Dynatrace Diagnostics besitzt eine einfache, aber dennoch effiziente Struktur (Abb. 1).

Virtuelle Maschinen mit Anschlüssen

Recht früh haben die Entwickler der Java Virtual Machines (JVM) die Notwendigkeit einer standardisierten Schnittstelle erkannt, an der Informationen für Entwicklungs- und Monitoring-Tools bereitstehen, etwa für Debugger, Coverage-Tools oder Profiler. Bis Java 1.4 waren es das JVM Profiling Interface (JVMPI) und das JVM Debug Interface (JVMDI), die ab Java 5 zum JVM Tool Interface (JVMTI) zusammenwuchsen. Entsprechende Schnittstellen sind für Microsofts Common Language Runtime (CLR) vorgesehen. Einstiegspunkte bieten die Profiling-API (insbesondere *ICorProfilerInfo* und *ICorProfilerCallback*) sowie weitere, beispielsweise die Debug- und die MetaInfo-API, die den Zugriff auf weitere Interna der CLR erlauben.

Über die Schnittstellen kommt man an die Zustandsinformationen der virtuellen Maschine heran und erhält die Kontrolle über die dort laufenden Applikationen. Der Ablauf ist einfach: Ein Tool meldet sich als Agent am Interface an und erhält so im Kontext der Applikation Informationen über die gewünschten Ereignisse. Events erzeugt die VM für alle relevanten Laufzeitereignisse, für den Start und Stopp, das Laden von Klassen, Ein- und Austritte von Methoden, Exceptions, für alle Speicheroperationen wie Heap Allocations oder Objektfreigaben durch den Garbage Collector sowie für das Starten und Stoppen von Threads.

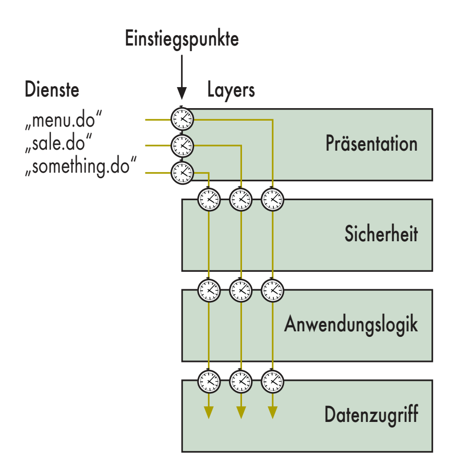
Die Benachrichtigung über Ein- und Austritt einer Methode führt allerdings zu einem hohen Performance-Schwund, vor allem weil die VM für alle Methodenaufrufe bis in Basisklassen hinein ein solches Event generiert. Diesen Overhead bekommt man nur durch gezielte, bedarfsorientierte Methodeninstrumentierung in den Griff. Der richtige Zeitpunkt dafür ist das Laden einer Klasse in den Speicher beziehungsweise der Aufruf des Just-in-time-Compilers.

Inzwischen zählt die Bytecode-Instrumentierung zu den festen Bestandteilen der Tool-APIs für VMs, nicht nur bei JVM und .Net. Bei Java stellt die „Byte Code Engineering Library“ einen Quasi-Standard dar, auf die diverse Profiler, Tracing-Tools und AspectJ zurückgreifen. Microsoft bietet für seine CLR, als Teil der *ICorProfilerInfo*-Schnittstelle, Methoden zur Instrumentierung der Intermediate Language (IL).

Als Testumgebung dienten typische 3-Tier-Architekturen, wie sie im Unter-

iX-TRACT

- Dynatrace Diagnostics bietet dem Anwender Funktionen sowohl zum Performance-Management als auch zur Fehlerdiagnose.
- Dabei kann Diagnostics den Datenfluss über mehrere Server hinweg sowohl durch Java- als auch durch .Net-Applikationen verfolgen.
- Dazu installiert Diagnostics sogenannte Agents auf den infrage kommenden Systemen, die über ihre Knowledge Sensors in den Applikationen Rohdaten erfassen.
- Über die grafische Oberfläche des Diagnostics Client kann der Anwender die Komponenten konfigurieren sowie die vom Diagnostics Server grafisch und statistisch aufbereiteten Daten analysieren.



Der wahre Weg: Purepath durchläuft die typischen Schichten einer Anwendung (Abb. 2).

nehmensumfeld oft vorzufinden sind. Die Nutzer greifen über Webclients auf die eigentliche Anwendung zu, die aus einem verteilten Web- und Applikationsserver besteht. Oft sind zusätzlich Datenbanken, SAP oder Legacy-Systeme in die Anwendung integriert. Das lässt erahnen, wie heterogen die Umgebungen sind und vor welche komplexen Aufgaben das die Systemadministration stellen kann.

Um Diagnostics erproben zu können, enthielt die Testumgebung typische Störfälle etwa bedingt durch ungünstige Konfigurationen der Anwendungen (zu kleine Pools und Verbindungen), der Software (Thread-Synchronisation, CPU-intensive Methode) und des Netzes (hoher Latenz). Es kamen zwei Architekturen mit passenden Anwendungen für den Test zum Einsatz:

– Die von Microsoft im MSDN für Entwickler angebotene .Net-Anwendung Pet Shop 3.0, bei der alle drei Tiers auf einem Server installiert waren. Der Zugriff der Benutzer erfolgte über Webbrowser.

– Die J2EE-Anwendung Day Trader, verteilt auf einen Applikations- und Webserver unter Linux sowie auf einen MySQL-Datenbankserver unter Windows 2003. Als Clients dienten nativ in Java oder .Net implementierte Programme unter Windows XP.

Bei der Durchführung eines Lasttests der Anwendungen im Unternehmensumfeld simuliert man eine große Anzahl paralleler Client-Zugriffe und misst Größen wie Antwortzeiten und Transaktionsdurchsatz. Die dazu verwendeten Hilfsmittel, beispielsweise HPs Loadrunner, Empirix eLoad oder Borlands Silkperformer, führen dazu Blackbox-Tests durch. Ist die Leistung des Systems nicht zufriedenstellend, geben sie keinen Hinweis auf die Ursachen, ein Monitoring der Komponenten CPU, Disk- oder Netzwerkauslastung der beteiligten Rechner ist damit aber fast immer realisierbar. Da Diagnostics in der vorliegenden Version 2.6.0 (noch) keine Systemmonitoring-Daten liefert und sich auf die Applikationen beschränkt, wäre es hilfreich, die Daten beider Werkzeugarten kombinieren zu können, damit man einen optimalen Gesamtüberblick bekommt. Dynatrace Diagnostics bietet ebenso wenig wie alle anderen kommerziellen Tools hierfür Schnittstellen an. Somit muss man in der Analysephase immer wieder hin- und herspringen.

Einstiegspunkt per Lastanalyse finden

Einen ersten Gesamtüberblick der Durchsatzraten, Antwortzeiten und Systemauslastung aus Nutzersicht liefert ein Lasttest-Werkzeug. Auf Basis dieser Daten rückt man den Engpässen mit Dynatrace Diagnostics zu Leibe. Im Falle der Webanwendung im Test ist der Einstieg über den View „Tagged Web Requests“ naheliegend, in dem in einer tabellarischen Ansicht die „Einstiegspunkte“ der Clients in die Anwendung aufgelistet sind. Hat man in seine Testskripte passende Tags für den Loadrunner eingebaut, tauchen sie unter ihren Namen in den in Diagnostics gelisteten Webabfragen wieder auf.

Zu jedem Request findet man einige Messwerte wie die übertragene Datenmenge, CPU-Zeiten oder insgesamt dafür verbrauchte Zeit. Das reicht oft, eine typische Schwäche im System wie inakzeptable Antwortzeiten für den Nutzer zu entdecken. Für die weitere Analyse bis hinunter auf die Codeebene kommt Purepath ins Spiel. Der Analytiker kann an jedem Punkt entscheiden, ob er weiter ins Detail gehen (über Method-Breakdown beziehungsweise Purepath) oder, falls er beim Detail angekommen ist, die Summe über alle Methoden-APIs auf dieser Ebene bekommen will.

Im Test fielen die veränderten Methoden der Applikationen sofort auf, die Dinge simulieren sollten wie rechenintensive Prozeduren oder mangelnde Synchronisation. Hat man nach erfolgreicher Identifikation eine potenzielle Verbesserung im Code vorgenommen, kann man in den Darstellungen des Diagnostic Client Testläufe miteinander vergleichen. Softwarearchitekten erkennen leicht, an welchen Stellen es tatsächlich messbare Veränderungen gab. Dabei hilft ihnen Diagnostics, indem es ihnen den direkten Sprung an die entsprechende Stelle im Quellcode der aufgeführten Packages, Klassen oder Methoden erlaubt, sofern die Entwickler Eclipse oder Visual Studio genutzt haben.

Für Auswertungen etwa mit ANOVA oder DoE (Design of Experiment) aus der „Six Sigma Welt“ fehlt eine Exportfunktion für die Einzelmessungen zur Analyse mit Programmen wie Minitab oder Fathom. Bis dato müssen sich Statistiker mit im 10-Sekunde-Raster generierten Min-, Max- oder Mittelwerten begnügen. Exportieren kann man in Diagnostics über CSV und HTML oder die JMX-Schnittstelle.

Weil der Analyseschwerpunkt von Dynatrace auf der Softwareseite liegt – was in Entwicklungsabteilungen si-

Editionen

Dynatrace Diagnostics

Workstation Edition: erlaubt die Analyse des Applikationsverhaltens einer Anwendung während der Softwareentwicklung in der lokalen Entwicklungsumgebung.

Professional Edition: bietet zusätzlich die Überwachung und Diagnose von zwei produktiven Applikationen tagtäglich rund um die Uhr.

Enterprise Edition: Überwachen, Diagnostizieren und Performance-Management sämtlicher Applikationen im Betrieb inklusive Java-Anwendungen auf dem Mainframe, Zugriff auf Diagnosedaten und Aktionen unternehmensweit.

Preise: auf Anfrage, www.dynatrace.com

iX-Wertung

⊕ Echtzeitanalyse von Business-Transaktionen mittels Purepath

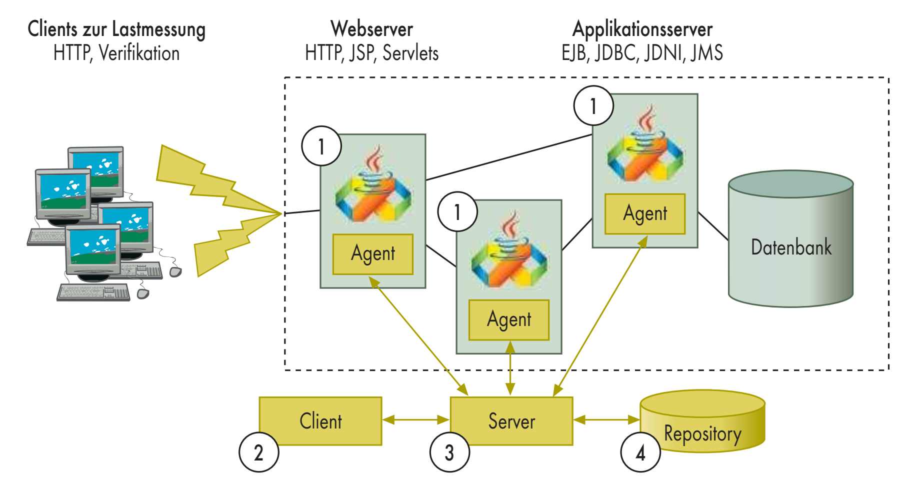
⊕ systemübergreifender Einsatz

⊕ Analyse im gesamten Entwicklungszyklus

⊖ .Net-Unterstützung hinkt der von Java hinterher

⊖ keine Einbindung von älteren und nativ implementierten Komponenten

⊖ beschränkte Exportfunktion der Messdaten



Testaufbau: Die an den Messpunkten (1) von den Agenten gesammelten Daten erscheinen vom Server (3) grafisch aufbereitet auf dem Client (2) und können im Repository (4) hinterlegt werden (Abb. 3).

cherlich gefragter ist – ließen sich andere im Test bewusst eingebaute Bremsen, etwa eine limitierte Anzahl von gleichzeitig erlaubten Browser-Verbindungen zum Webserver, besser durch die Analyse mit dem Lasttest-Tool identifizieren. Das hat Dynatrace wohl erkannt und für die kommende Version 3.0 Erweiterungen für das System-Monitoring angekündigt.

In den Tiefen der Applikation

Ob man als Performance Engineer Bottlenecks identifizieren will oder als Entwickler auf Fehlersuche ist, man profitiert von Diagnostic. Aber auch Systembetreuern hilft es, wenn sie das dynamische Verhalten eines in Betrieb befindlichen Systems beobachten, verstehen und verifizieren wollen. Sie erhalten durch die Echtzeit-Analyse eine Unterstützung, bei der die Messwerte des „System under Diagnose" (SUD) mit geringer Verzögerung ständig beim Diagnostics Client eintreffen. JMX erlaubt für einige Messvorgänge die Anbindung an Frameworks wie IBMs Tivoli oder CA Unicenter.

Als Einstieg empfiehlt sich ein Discovery Run, bei dem die Applikation möglichst realistische Anwendungsfälle durchläuft. In typischen Enterprise-Architekturen kann man mit dem mitgelieferten Sensor Pack von Dynatrace, das standardmäßig alle gängigen Techniken unterstützt, Analysen durchführen. In der Grobarchitektur Server, Applikationen und Software-Layer tritt über die aufgezeichneten Purepathes das dynamische Zusammenspiel der Komponenten/Layer und deren Kommunikationsschnittstellen zutage.

Damit erlangt man in kürzester Zeit einen Überblick, selbst bei komplexen oder wenig bekannten Architekturen. Der Schritt kann zu überraschenden Erkenntnissen vor allem bei besonders fantasievollen Implementierungen führen. Positiv fällt auf, dass Systemgrenzen oder Herstellereigenheiten weitgehend transparent bleiben und Dynatraces Tools die Analyse von Transaktionen nicht behindern.

Wer tiefer in die Applikation eintauchen will, kann im Dynatrace-Client eigene erweiterte Konfigurationen vornehmen und auf dem Server persistent hinterlegen. Der Anwender der Werkzeuge darf im während des Discovery Run „erlernten" Klassenbaum auf Methodenebene Sensoren an- oder abwählen.

Alternativ zum eben beschriebenen Weg „Outside-in", unterstützt Dynatrace ein „Inside-out": Ausgehend von Exceptions oder identifizierten Engpässen auf Methodenebene, kann man die zugehörigen Business-Transaktionen identifizieren und damit die eventuell finanzielle Auswirkung verstehen.

Obwohl Dynatrace alle gängigen Techniken und Hersteller unterstützt, stößt man im praktischen Einsatz an Grenzen, insbesondere wenn ältere oder nativ (in C/C++) implementierte Komponenten wesentlicher Bestandteil des Systems sind. Analysen von Vorgängen auf dem Datenbankserver (etwa bei Stored Procedures) oder dem SAP-Backend sind nur über proprietäre Tools durchführbar. Diagnostics erfasst aber immerhin die Aufrufschnittstelle einschließlich ihrer Parameter, was für eine erste Analyse ausreichen dürfte.

Trotz der breiten Zielgruppe, die Dynatrace ansprechen möchte, bleibt die Benutzbarkeit nicht auf der Strecke. Sowohl das Konfigurieren als auch das Erfassen und Auswerten von Messwerten nebst Traces ist intuitiv durchführbar und erlaubt flüssiges Arbeiten. Bei komplexen Systemen kann man zwar durch die Vielzahl der Fenster leicht die Übersicht verlieren, kommt aber über das Cockpit schnell wieder zurück zum Ausgangspunkt, egal ob das ein Purepath, ein Web Request oder eine Exception war. Ohne Hindernisse funktionierte das verteilte Arbeiten mit Dynatrace, das gerade im Enterprise-Umfeld ein Muss ist. Der Client regiert auch aus der Ferne selbst über schmalbandige Verbindungen schnell genug. Daten stehen sowohl online als auch „aus der Konserve" offline zur Analyse zur Verfügung. Das ist besonders praktisch, wenn die Auswertung durch ein anderes Team erfolgt oder sogar über mehrere Zeitzonen geht.

Fazit

Wer jemals versucht hat, in verteilten Systemen ein rudimentäres Messsystem zu implementieren, das es erlaubt, die beteiligten Komponenten bei Performance- und Stabilitätsproblemen synchronisiert für eine Auswertung unter einen Hut zu bekommen, für den dürfte Dynatrace Diagnostics eine spürbare Erleichterung sein. Auch wenn es andere spezifische Tools nicht vollkommen ersetzen kann, bietet es wegen seiner Systemunabhängigkeit und dem breiten Anwendungsspektrum vor allem für Teams eine passende Analysegrundlage. Bei der Untersuchung der Anwendung erlaubt Dynatraces Purepath-Technik einen tiefen und frei wählbaren Einblick. (rh)

FRANK ROMETSCH

ist Senior Engineer bei Siemens Corporate Technology. Seine Themenschwerpunkte sind Softwaretest und Performance Engineering.

HORST SAUER

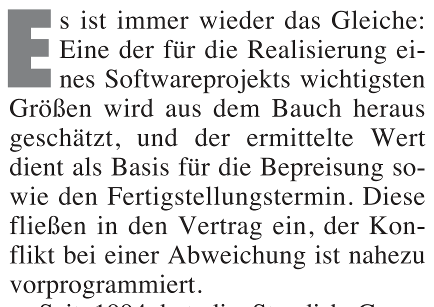
ist Senior Engineer bei Siemens Corporate Technology. Seine Themenschwerpunkte sind Softwaretest, Testbarkeit und Diagnose.

Aufwand, Zeit und Kosten mit Cost Xpert schätzen

Zur Sache, Schätzchen

Frank Müller

Um die Kosten für ein geplantes Projekt realistisch einzuschätzen, muss man mehr berücksichtigen als nur den zu erwartenden Code-Umfang und die dafür benötigte Zeit. Risiken, mögliche Fehler und der – häufig vernachlässigte – Aufwand für die Dokumentation gehören ebenso dazu wie der Wissensstand der Mitarbeiter. Cost Xpert soll dabei helfen, die Fülle der zu bedenkenden Größen in den Griff zu bekommen.



Es ist immer wieder das Gleiche: Eine der für die Realisierung eines Softwareprojekts wichtigsten Größen wird aus dem Bauch heraus geschätzt, und der ermittelte Wert dient als Basis für die Bepreisung sowie den Fertigstellungstermin. Diese fließen in den Vertrag ein, der Konflikt bei einer Abweichung ist nahezu vorprogrammiert.

Seit 1994 hat die Standish Group International, Inc. über 100 000 Projekte in den USA auf ihren Erfolg in Bezug auf Umfang, Zeit, Kosten und Qualität hin überprüft. Ergebnis ist der alle zwei Jahre erscheinende Chaos Report, der diese Projekte in drei Kategorien einteilt: Die erste ist „successful“ und gilt für die Projekte, die alle Anforderungen erfüllen sowie in Zeit und Budget liegen. Als „challenged“ gelten solche, die abgeschlossen wurden und im Einsatz sind, deren Entwicklung jedoch in Zeit, Budget oder Leistung nicht im vorgesehenen Umfang lag. In der letzten Kategorie hat man die Entwicklung abgebrochen oder das Ergebnis nie eingesetzt. Solche Projekte gelten als „failed“. Im Verlauf der Jahre 1994 bis 2006 hat sich der Anteil erfolgreicher Projekte von 16 auf 35 Prozent erhöht – ein positiver Verlauf, der jedoch nicht von den 65 Prozent der unplanmäßigen oder gescheiterten Vorhaben ablenken darf.

Für die Fehlschläge gibt es sicherlich eine Vielzahl von Gründen. Diese sind nur selten technischer Natur, sondern liegen im Projektmanagement und dem Entwicklungsprozess mit seinen Bestandteilen. Einer dieser Bestandteile ist das Schätzen des Aufwands, also die Bestimmung der Zahlen, die Aussagen, wie viel Zeit die Realisierung eines Projekts benötigt und welche Personalkosten zu erwarten sind. Neben der Preisgestaltung, die natürlich aus strategischen Gründen von den kalkulierten Kosten abweichen darf, dienen diese Informationen zur Bestimmung der Größe des Projektteams und der Festlegung des Terminplans. Fehler wirken sich also immer auf den Projekterfolg aus.

Entscheidungen aus dem Bauch heraus

Die von allen Beteiligten für das Angebot und die Planung geforderte präzise Schätzung erstellt der Projektleiter oder der Seniorentwickler häufig wenig formal aus dem Bauch heraus. Historische Daten für eine Justierung liegen nicht vor oder er zieht sie nicht heran, Parameter wie die Qualität des Entwicklungsprozesses, die noch nicht geklärte Verfügbarkeit fachlich und technisch versierter Entwickler oder der Einfluss eines möglichen Zeitdrucks sind nicht Bestandteil seiner Überlegungen, und selbst bei Großprojekten setzt man häufig keine aktuellen Techniken zur Aufwandsabschätzung ein.

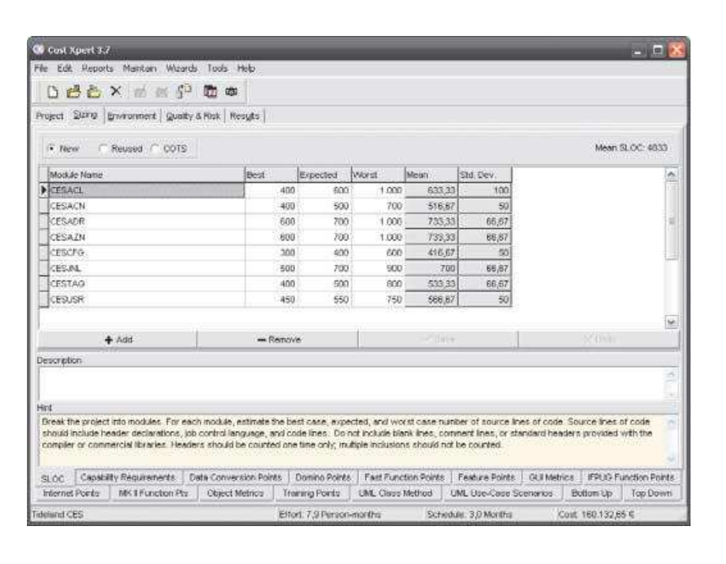
Ein etabliertes Modell für die Abschätzung von Aufwand, Kosten und Zeit mithilfe mathematischer Funktionen heißt Constructive Cost Model II (COCOMO II). Auf der Website des Center for Systems and Software Engineering (csse.usc.edu) sind mehrere frei verfügbare Tools zu finden, die diese Methodik unterstützen. Darüber hinaus gibt es Links auf zwei kommerzielle Werkzeuge. Eine davon ist Cost Xpert, deren vor Kurzem freigegebene Version 3.7 dem Autor zum Test vorlag. Die Cost Xpert Group mit Sitz in Augsburg ist ständiges Mitglied der Forschungsgruppe COCOMO II und hat sich auf die Entwicklung einer Methodik für die Aufwandsabschätzung sowie eines Werkzeugs für diesen Zweck spezialisiert. Cost Xpert soll den Schätzer von der Erfassung initialer Projektdaten über Größen, Umgebung, Qualitäts- und Risikojustierung bis zum Ergebnis mit einer Vielzahl von Auswertungen begleiten. Der Test sollte zeigen, wie viel Arbeit die Software dem Anwender wirklich abnimmt und inwieweit sie zu einem realistischen Resultat gelangt.

Zu Beginn einer Aufwandsberechnung legt der Anwender den Namen des Projekts und sein Anfangsdatum fest. Ausgehend von diesem Datum soll ermittelt werden, zu welchen Zei-

ten welche Mitarbeiter für welche Aufgaben benötigt werden, sodass Cost Xpert schließlich die optimale Teambesetzung über die Laufzeit ausgibt. Weiter geht es unter dem Label „Project Method“ mit der Auswahl des Projekttyps, des Lebenszyklus sowie eines Standards für die auszuliefernden Artefakte. So lässt sich beispielsweise definieren, dass eine E-Commerce-Anwendung iterativ-inkrementell entwickelt wird. Dabei kann man bereits diverse Koeffizienten, typische Risiken sowie Defektraten anpassen. Die Anwendung gibt hier schon hilfreiche Daten vor, zum Beispiel 48 typische Lebenszyklen, und unterstützt mit einem Wizard. Der unbefangene Einsteiger ist jedoch überrascht, welche den Aufwand beeinflussende Vielfalt schon hier zu beachten ist.

Der nächste Schritt befasst sich mit finanziellen Parametern, wie den Anteilen für die Systemintegration, Maintenance und Gehaltsentwicklung sowie den Stunden pro Personenmonat für eine korrekte Berechnung. Weiter geht es mit den Stundensätzen für unterschiedliche Rollen und der Definition, welche Sprachen mit welchem Anteil zum Einsatz kommen. Letzteres ist für die Umrechnung von Eingangsgrößen in Source Lines of Code (SLOC) relevant, da diese für die weiteren Berechnungen als wichtiger Eingangswert dienen. Ein weiterer Tab erlaubt die Erfassung tatsächlicher Aufwandsdaten nach Abschluss des Projekts, die jedoch nur gespeichert werden und in keine automatische Kalibrierung einfließen. Die Speicherung muss der Anwender manuell vornehmen. Mit der Eingabe von Kontaktdaten ist der Start abgeschlossen, die eigentliche Abschätzung beginnt.

Unter dem Titel „Sizing“ stehen dem Schätzer 16 Methoden zur Bestimmung der Softwaregröße zur Verfügung. Die erste direkte Methode bildet die direkte modulare Eingabe der Source Lines of Code. Diese werden wie alle weiteren Schätzungen jeweils unter den Kategorien „optimistisch“, „pessimistisch“ und „erwartet“ erfasst. Neben der Neuerstellung kann der Anwender eine Wiederverwendung vorhandenen Codes sowie den Einkauf kommerzieller Lösungen bewerten, unterstützt durch Hilfstexte und einen Wizard.



Bei der Bestimmung der Eingangsgrößen kann der Anwender zwischen optimistischer, pessimistischer und erwarteter Schätzung differenzieren (Abb. 1).

Beeinflussung durch viele Faktoren

Die weiteren Sizing-Eingaben folgen einem ähnlichen Muster und ziehen unterschiedliche Methoden heran: Capability Requirements, Data Conversion Points, Domino Points, Fast Function Points, Feature Points, GUI Metrics, IFPUG Function Points, Internet Points, Mk II Function Points, Object Metrics, Training Points, UML Class Method, UML Use Case Scenarios, Bottom Up und Top Down. Je nach Projektart und Erfahrung wird hier jeder fündig. Dabei kann man mehrere Eingangsgrößen leicht in der Gesamtberechnung kombinieren.

So schön sich die Anzahl unterschiedlicher Eingangsgrößen darstellt, so sehr fehlt hier jedoch eine Unterstützung des Schätzers bei der Bestimmung der angegebenen Werte. Dies geht natürlich nicht überall, jedoch ist die Angabe beispielsweise von IFPUG Function Points nicht gerade trivial. An dieser Stelle würde eine modulare Erfassung inklusive eines Wizard für Standardsituationen helfen. Auf diese Weise würden alle Eingangsgrößen innerhalb von Cost Xpert verwaltet werden.

Hat man den Umfangs des zu erstellenden Codes festgestellt, ist bereits eine Menge geschafft. Nun ist dies jedoch, wie oben angedeutet, nicht die einzige Größe, die den Aufwand eines Projekts festlegt. Das Constructive Cost Model II (COCOMO II, siehe *iX*-Links), ein etabliertes Modell zur Abschätzung von Aufwand, Kosten und Zeit, konzentriert sich auf eben diese Faktoren. Als Eingangsgröße fungieren hier die Source Lines of Code, die Bestimmung dieser Anzahl ist nicht Bestandteil des Modells. Je nach Submodell werden unterschiedliche Parameter auf diesen Wert angewandt. Dies sind die exponentiell wirkendenden Scaling Factors sowie die linear wirkenden Product, Platform, Personnel und Project Factors. Im Post-architecture Submodell addieren sie sich auf insgesamt 22 Faktoren. Diese finden sich bei Cost Xpert unter dem Titel „Environment“ wieder. Das Werkzeug geht jedoch differenzierter vor und unterscheidet zwischen 43 Faktoren.

Jeder dieser Faktoren bewegt sich wie COCOMO II in sechs Stufen zwischen „very low“ und „extra high“, einige verfügen über eine geringe Auswahl. Die Scaling Factors decken sich mit dem Vorbild und umfassen die Bewertung des Designs hinsichtlich potenzieller Risiken sowie der Einplanung von Gegenmaßnahmen, der möglichen Flexibilität in der Entwicklung, der Vergleichbarkeit dieses Projekts mit zuvor realisierten Vorhaben, der Reife des Entwicklungsprozesses gemessen am CMM Level (Capability Maturity Mo-

iX-TRACT

- Ungenaues Schätzen der für ein Projekt anfallenden Kosten und des benötigten Personalaufwands trägt häufig dazu bei, dass ein Projekt nicht erfolgreich im geplanten Zeitraum beendet wird.
- Die Ungenauigkeit bei der Schätzung ist darauf zurückzuführen, dass die Projektverantwortlichen eine große Anzahl unterschiedlicher Faktoren berücksichtigen müssen, deren Relevanz und Umfang sie oft nach Gefühl bewerten.
- Cost Xpert ist ein Werkzeug, das auf der Basis einer für die Aufwandschätzung entwickelten Methodik, mit zum Teil vorgegebenen Eingangsgrößen und vielfältigen Kategorien den Projektverantwortlichen interaktiv bei seiner Planung unterstützt.

del) sowie das gemeinsame Verständnis zwischen Beteiligten über die Projektziele. Wizards helfen hier wieder bei einer korrekten Einstufung.

Weiter geht es mit Faktoren zur Bewertung von Daten bei Migrationsprojekten. Dazu zählen beispielsweise die Fehlertoleranz, die Qualität der Quelldaten und der Anteil der zu konvertierenden Daten. Auch die Rahmenbedingungen der Plattform bestimmen den Aufwand. Hierunter fallen der zur Verfügung stehende Anteil an Rechenzeit und Hauptspeicher sowie die Flüchtigkeit bei Hardware, Betriebssystem, Datenbanken und weitere externe Systembestandteile.

Wichtig und dennoch immer wieder unterschätzt ist der Einfluss personenbezogener Faktoren. Zu diesen gehören die Fähigkeit von Analysten, die Erfahrung bezüglich der fachlichen Domäne sowie mit Sprachen und Werkzeugen, die Unterstützung durch das Management, die Erfahrung des Managements, die Stabilität in der Besetzung, die Erfahrung mit der Plattform sowie die Fähigkeiten der Entwickler. In der Regel wird angenommen, dass der Wissensstand aller Projektbeteiligten dem fortgeschrittener Entwickler oder der Projektmanager entspricht.

Einer weiteren Gruppe widmet Cost Xpert der Aufgabenverteilung. Sie umfasst die Erledigung von Arbeiten durch Einzelpersonen, kleine oder größere Teams, die Verteilung von Mitarbeitern auf mehrere Projekte gleichzeitig und die Möglichkeit, sich einem Thema konzentriert widmen zu können. Im Rahmen der Projektbewertung wird der effektive Einsatz von Managementwerkzeugen und die Entwicklung an einem oder mehreren Standorten eingeschätzt. Bei Letzterem fließt auch ein, welche Hilfsmittel die Kommunikation bei einem verteilten Projekt unterstützen. Die Projektfaktoren gehen jedoch noch weiter. Nicht unerhebliche Parameter sind die Ausgestaltung des Arbeitsplatzes und der Einsatz moderner Entwicklungsumgebungen sowie unterstützender Werkzeuge. Beim zu entwickelnden Produkt selbst ist nicht nur die fachlich bestimmte Größe ein zu betrachtendes Kriterium. So fließen die Datenbankgröße im Verhältnis zum Code-Umfang, Anforderungen an die Dokumentation des Lebenszyklus, Internationalisierung, Komplexität der Berechnungen und Operationen, Anforderungen an die Wiederverwendung und die erforderliche Zuverlässigkeit ebenfalls mit ein.

Bei Internet-Projekten greift eine eigene Gruppe von Faktoren. Diese umfassen den Einsatz von Grafik und Multimedia, die Integration von Legacy-Anwendungen, Anforderungen an die Sicherheit, Content, Werkzeuge, zu erwartende Transaktionslasten und das Vorhandensein einer Webstrategie. Zu guter Letzt sind die Einflüsse von Trainingsprojekten in der Aufwandskalkulation zu berücksichtigen. Hierzu zählen die Erfahrung des Ausbilders, die Größen der Klassen sowie das erforderliche Ausbildungsmaterial. Obwohl viele dieser Faktoren in einer Reihe von Projekten auf dem Standard „nominal“ belassen werden können, zeigt die Liste doch, worüber sich der Schätzer Gedanken machen sollte. Der Entwicklungsaufwand hängt eben nicht nur vom Umfang der fachlichen Anforderungen ab, sondern wird zusätzlich von Produktcharakteristiken und den Entwicklungsbedingungen beeinflusst.

Kurz vor dem Ziel

Neben der Bewertung der einfließenden Faktoren gibt es weitere Präferenzen, die den Aufwand eines Projekts und seine Dauer beeinflussen. Ihnen hat Cost Xpert eine eigene Kategorie gegönnt. Mittels diverser Schieberegler sowie einem Eingabefeld kann der Schätzer definieren, ob es eher auf eine Zeit- oder eine Kostenoptimierung ankommt und ob die maximale Anzahl der Mitarbeiter beschränkt ist. Aus Sicht des Projektplans erfasst die Software, wie klar die Anforderungen sind, wie viel Zeit für Integration und Tests das Team einplanen soll und wie hoch die Überlappung einzelner Arbeiten sein kann. Letzteres ist bei größeren Teams mit dedizierten Rollen leichter möglich als in kleinen Projekten. Ein weiterer Regler bestimmt den Einfluss durch sich verändernde beziehungsweise erweiternde Anforderungen. Im Rahmen der Risikobetrachtung kann man zusätzlich zu den bis dahin geschätzten Kosten eine Rückstellung erfassen sowie das Risiko einer Fehlplanung einstufen. Letztlich wird noch die Interaktion mit dem Kunden durch die Angabe von dessen Antwortzeit bewertet.

Durch die Regler kann der Anwender diese Werte fein gestuft eingeben, feiner als es die sechs Stufen der Faktoren vorgeben. Die Software zeigt Aufwand, Zeit und Kosten in der Statuszeile an, sodass der Anwender den Einfluss, den sie haben, unmittelbar ablesen kann. Das lädt zum Experimentieren ein und gibt hilfreiches Feedback für eine realistische Planung. Detailliertere Informationen zu den einzelnen Posten liefert die Kategorie „Results“.

Neben einer Übersicht als Einstieg finden sich Tabellen mit den Werten zu den individuellen Tätigkeiten, zu Risiken, zur Verteilung der Arbeit unterschiedlicher Rollen über die Zeit, Kalkulationen zu Teamgrößen und Defekten im Rahmen der Wartung sowie auszuliefernde Artefakte. Nahezu alle Werte lassen sich zusätzlich als Grafiken ausgeben, die für eine Weiterverarbeitung exportiert werden können. Diese Fähigkeit gilt auch für einige der Ergebnistabellen, die so ihren Eingang in MS Project, MS Excel, CSV, PDF oder HTML finden. Alternativ lassen sich umfangreiche Reports generieren.

Für die Berechnung der Ergebnisse zieht Cost Xpert eine Vielzahl von Werten und Faktoren heran, die das Werkzeug als Basis mitbringt. Über den Menüpunkt „Maintain“ kann der Schätzer sie für sein eigenes Umfeld justieren. Hierzu bedarf es einer Kultur von Projektanalysen, bei denen Anfangsschätzungen mit den tatsächlichen Ergebnissen abgeglichen werden, sodass sich mit der Zeit nicht nur sein eigenes Schätz-Know-how verbessert, sondern eben diese Eingangswerte eine Anpassung erfahren. Hierzu gehören Projekttypen, Lebenszyklen, die Umrechnung von Funktionspunkten auf SLOC, Risiken, Aufgabenaufteilung oder die Faktoren.

Weitere Werkzeuge helfen dem Schätzer bei seiner Arbeit. Neben integrierter Wizards für Details bietet Cost Xpert eine Reihe hilfreicher „Zauberer“ für einen schnellen Einstieg. Diese liegen für das Projekt, die Eingangsgrößen, die Umgebung sowie Qualitäts- und Risikoparameter vor. Mehrere parallele Projekte im Verantwortungsbereich des Schätzers lassen sich durch ein Portfolio gemeinsam verwalten und kumulieren. Snapshots und Baselines helfen bei

Daten und Preise

Cost Xpert 3.7

Hersteller: Cost Xpert AG, www.costxpert.de

Softwarevoraussetzungen: Windows 98, 2000, NT, XP 2003, Vista

Preis: Cost Xpert: 2350 €
Wartung (inkl. Upgrade): 720 €/Jahr

iX-Wertung

⊕ vielfältige Bestimmung der Eingangsgrößen

⊕ umfangreiche Umgebungsparameter und Vorgaben

⊕ gute Benutzerführung

⊖ eingeschränkte Modularität der Eingangsgrößen

⊖ heterogene Projekte lassen sich nur über Portfolio abbilden

der Berechnung von Alternativen und dem späteren Vergleich.

Fazit

Zugegeben, die Arbeit mit Cost Xpert ist komplex. Dies liegt jedoch nicht an der Software, sondern an der Aufgabenstellung. Die Feststellung des Realisierungsaufwands für ein Projekt setzt sowohl Erfahrung als auch Sorgfalt und die richtige Technik voraus. Hierbei fungiert Cost Xpert als hilfreiche Unterstützung, die langjähriges Wissen zusammenfasst. Das Programm führt den Schätzer sequenziell durch alle Schritte, die zu bedenken sind. Gleichzeitig wird er jedoch nicht so durch Wizards eingeengt, dass er keine Abkürzungen nehmen oder keine zwischenzeitlichen Erkenntnisse erfassen kann. Die vielfältigen Möglichkeiten zur Bestimmung der Eingangsgrößen gefallen ebenso wie die umfangreichen Umgebungsfaktoren und Projektvorgaben.

Als Wünsche bleiben eine Möglichkeit, Eingangsgrößen wie Funktionspunkte modular und für Standardsituationen durch Wizards unterstützt zu erfassen sowie die Verwaltung heterogener Projekte mit Teilprojekten. Diese könnten sich dann im Sprachmix sowie den Faktoren unterscheiden. Heute lässt sich dieses über Portfolios teilweise abbilden.

Bei aller Unterstützung darf man jedoch eines nicht vergessen: Wie es das Wort bereits ausdrückt handelt es sich weiterhin um eine Schätzung, keine absolute Berechnung. Erst im Verlauf eines Projekts nimmt mit der Sicherheit über Anforderungen und Umgebung auch die Qualität der Abschätzung zu. Eine Verbesserung gegenüber einer einfachen Bauchschätzung ist ein formales Vorgehen jedoch immer. (ka)

FRANK MÜLLER

arbeitet als Teamleiter und Senior Consultant bei der BTC Business Technology Consulting AG in Oldenburg.

Literatur

[1] Capers Jones; Social and Technical Reasons for Software Project Failures; STSC CrossTalk June 2006 Issue; www.stsc.hill.af.mil/crosstalk/2006/06/0606Jones.html

[2] Capers Jones; Software Cost Estimating Methods for Large Projects; STSC CrossTalk April 2005 Issue; www.stsc.hill.af.mil/crosstalk/2005/04/0504Jones.html









Bibliothek jQuery:
Ajax und Animation erleichtert

Wenig schreiben

Markus Franz

Besonders im Ajax-Umfeld sind Javascript-Bibliotheken Legion. Mit jQuery liegt ein schlankes Framework für Entwickler vor, denen andere zu weitreichend sind.

Javascript ist ein wesentlicher Bestandteil des Web 2.0. Die Sprache ist dynamisch, kümmert sich kaum um Datentypen und hat einen beeindruckenden Funktionsumfang. Von gestandenen Programmierern gelegentlich belächelt, lassen sich nur mit Javascript effizient Animationen, Übergänge und Ajax-Elemente in Webseiten realisieren. Und sie erfordert lediglich einen standardkonformen Browser.

Im Gegensatz zu manch anderer Programmiersprache kann man mit Javascript leicht schlechten Code schreiben. Es gibt eine unübersichtliche Standardbibliothek, zahlreiche Unterschiede der Implementierung im Browser, und die Dokumentation besteht oft nur aus Codeschnipseln. Hier setzen Javascript-Frameworks an, die strukturierte Schnittstellen für häufig benötigte Aufgaben bereitstellen: Die Verarbeitung von XML mit DOM, Animation, Ajax-basierte Oberflächen und vieles mehr. Besonders die XML-Bearbeitung mit dem DOM bereitet in Javascript keinen Spaß: Man muss zahlreiche Schleifen und wiederholende Statements schreiben.

Installation und Funktionen

jQuery (www.jquery.com) legt den Fokus auf hochwertigen, kurzen Quelltext. Es macht komplexe Anwendungen kompakter und reduziert so die Wartung der Applikationen durch den Programmierer. Skripte, die auf jQuery aufbauen, lassen sich leicht in anderen Anwendungen wiederverwenden.

Die aktuelle Version 1.2.3 des Framework ist nur rund 53 KByte groß. Es zu installieren fällt denkbar leicht: Man lädt die „Minified Version“ herunter und legt sie in einem Verzeichnis des Webservers ab. Die „Packed Version“ ist zwar deutlich kleiner (30 KByte), benötigt aber beim Laden auf dem Rechner des Anwenders einige Rechenleistung zum Dekomprimieren – bei jedem neuen Zugriff auf eine Webseite, die jQuery verwendet. Am oberen Ende der Bandbreite rangiert die unkomprimierte Version mit knapp 93 KByte. Die Minified Version liegt insgesamt wohl in der Mitte zwischen Größe und Geschwindigkeit sowie Bandbreite.

Mit Browsern ab Internet Explorer 6.0, Mozilla Firefox 1.5, Safari 2.0 und Opera 9.0 arbeitet die Bibliothek reibungslos zusammen. Sie bietet eine große Vielfalt an Funktionen: Neben einfachen DOM-Abfragen vereinfacht sie außerdem die XPath-Syntax zum Zugriff auf Inhalte in XML-Dateien, und sie kommt mit Selektoren aus CSS 3 zurecht, die das Rendering von HTML- beziehungsweise XML-Dateien für das jeweilige Ausgabemedium und Gerät gezielt steuern. jQuery kann definierte Events mit Aktionen belegen und Abfragen und Darstellung von Inhalten für Ajax verarbeiten. Unter Effects versteht das Framework die Animationen, die sich auf beliebige Dokumentelemente anwenden lassen.

Grundidee von jQuery ist es, eine Syntax zum Auffinden beliebiger Elemente (etwa aus dem DOM) zur Verfügung zu stellen. An den gefundenen Objekten können Programmierer beliebige Änderungen vornehmen. Der Einstieg in das Framework ist das Steuerzeichen *$*, im Grunde eine Javascript-Funktion. Man übergibt ihr einfach einen String, der als CSS-Selektor oder XPath-Ausdruck formuliert ist, und wählt so beliebige Elemente aus dem Dokument aus. Schon hier zeigt sich die Abkürzung, die jQuery in den Code einbringt. *$("#test");* kürzt das wesentlich längere Statement *document.getElementById ("test");* ab.

jQuery unterstützt eine große Untermenge der XPath-Syntax: Im einfachsten Fall wählt man mit *$("p")* alle *p*-Elemente aus. In der Komplexität ist jQuery mit XPath nach oben beliebig offen: Man kann beispielsweise alle Elemente finden lassen, die Kinder eines bestimmten Objekts sind („vater/kind“). Mit CSS-Selektoren steht die gewohnte Syntax bereit, Elemente im Dokument anzusprechen: *$("#test a")* weist das Framework an, nach allen Einträgen mit der ID *test* zu suchen. Danach sucht es alle Unterelemente *a* aus der zuvor ausgewählten Menge. Allgemein findet jQuery bei allen Abfragen immer alle

Einträge, sofern man nicht gezielt eine ID wie oben angibt.

Mehrere Abfragen lassen sich miteinander verbinden, da jeder Aufruf von *$* ein Objekt einer schon ausgeführten Abfrage entgegennehmen kann. So kann man sich gezielt im Dokument zum gewünschten Element hangeln und es weiterverarbeiten: Die Funktion *each()* geht durch eine Menge von Objekten und kann sie ausgeben. *$('p').each (function(i) { alert(this); });* etwa gibt den Inhalt aller *p*-Elemente aus.

Über die Funktion *css()* greift die Bibliothek auf die CSS-Eigenschaften zu und verändert sie: *$(„p“).css(„back ground-color“, „blue“);* färbt den Hintergrund aller Textabsätze blau. Versucht man, für dieses einfache Beispiel ein DOM-Äquivalent zu finden, reicht eine Zeile klassischer Javascript-Code nicht mehr aus. Nicht nur Stileigenschaften, sondern auch die Elemente selbst können über DOM verändert werden: Mit *append()* fügt man einem Knoten neue Inhalte hinzu.

Auf Ereignisse reagieren

Javascript kommt häufig zum Einsatz, wenn es darum geht, bestimmte Events zu behandeln: beim Laden der Webseite ein zusätzliches Fenster zu zeigen oder beim Überfahren eines Elements mit der Maus dies einzufärben. In jQuery kann man mit *ready()* definieren, dass eine Funktion nach dem Laden des HTML-Grundgerüsts auszuführen ist. *$(document).ready(func tion() {todo});* führt den Inhalt der Funktion aus, sobald das Dokument bereit ist. Es erzeugt ein Objekt, das es automatisch aufruft, sobald das HTML-DOM verfügbar ist. Ein mehrfaches *ready()* bewirkt das sequenzielle Ausführen der gewünschten Anweisungen. Wie so oft gibt es noch eine Abkürzung *$(function() {todo});* für das obige Statement.

Klickt der Besucher der Webseite einen Button mit der ID *mybutton* an, fängt jQuery diese mit *$("#mybutton").click(function() {todo});* einfach auf und ordnet ein Verhalten zu.

Ajax ist als technische Basis des Web 2.0 in aller Munde, aber es ist nicht ganz einfach, über Unterschiede der Browser hinweg einheitlichen Code zu schreiben. jQuery erleichtert dies. Die Funktionen *$.post()* und *$.get()* behandeln Aufrufe externer Programme auf dem Server. Die Funktionen bekommen dazu folgende Parameter übergeben:

– Das aufzurufende Skript sollte sich aus Sicherheitsgründen (muss aber nicht) auf demselben Server wie das Ausgangsdokument befinden.
– Die Argumente, mit denen das Skript aufgerufen werden soll, können Benutzereingaben oder der Inhalt eines Auswahlfelds sein.
– Eine optionale Callback-Funktion, die die Rückgabe des Servers entgegennimmt, die jQuery weiterverarbeiten kann.

```
$.post("speichern.php", { text: "kunde",
   number: 10}, function() { alert("Gespeichert!");
});
```

Dieser Code sendet einen Post-Request an *speichern.php* und übergibt die Inhalte *kunde* und die Zahl 10 als Argumente. Sobald die Abfrage abgeschlossen wurde, meldet die Callback-Funktion das dem Anwender.

Neben vielen anderen Funktionen für Ajax dürften Entwickler *load()* schätzen; diese Funktion fügt Inhalte eines Dokuments in ein ausgewähltes jQuery-Objekt ein. Der Code *$("#test"). load("test.html");* fügt *test.html* unterhalb des Elements mit der ID *test* ein. Die Beispiele sollten verdeutlicht haben, dass jQuery eine leistungsfähige Umgebung für Ajax-basierte Weboberflächen bietet. Einen genaueren Überblick über die Funktionen verschafft die Dokumentation (docs.jque ry.com), die recht umfangreich und mit guten Erklärungen sowie Codebeispielen vorliegt – allerdings nur in englischer Sprache.

Oft möchte man als Webentwickler nicht volles Ajax, sondern simple Animationen in das Dokument einbinden. jQuery bietet eine Reihe vordefinierter Effekte. Damit spart man sich komplizierte Berechnungen von Position, Höhe, Breite und Weg eines Objekts – das übernimmt alles das Framework.

Konkurrenz mit Prototype und anderen APIs

Die Funktionen *toggle()*, *slideUp()* und *animate()* lassen sich auf beliebige Elemente anwenden. Besonders Letztere ist interessant: Sie übernimmt als Argument ein Dictionary mit CSS-Eigenschaften, über die animiert werden soll. Der Befehl *$("#test").animate({width: 10, height: 10 });* verändert die Größe des angegebenen Elements auf 10 × 10 Pixel. Es steht hier die volle Bandbreite von CSS-Eigenschaften zur Animation zur Verfügung: Über Größe, Überlappung, Sichtbarkeit, Position und Farbe kann man ein Element beliebig anpassen. Seit der Version 1.2 unterstützt das Framework Animationen und Übergänge in Farben.

jQuerys bekannteste Konkurrenten sind Prototype, das Dojo-Toolkit und Rico. Die jeweiligen Stärken sind XML/DOM, Animationen, Ajax sowie JSON (Javascript Object Notation) und die Serialisierung von Objekten. Dabei haben die Konkurrenten jQuery unter anderem vordefinierte Kalender oder die automatische Vervollständigung von Benutzereingaben voraus. Und von Yahoo gibt es die gleichnamige User Interface Library, eine umfangreiche Sammlung von Javascript-Aktionen: vom Kalender bis Menüs und Logging.

jQuery bietet nicht allzu viel selbst vordefiniert an. Sucht man daher eine umfangreiche Funktionssammlung vordefinierter Elemente, liegt man bei jQuery falsch. Wer aber komplett eigene Anwendungen in Javascript entwickeln will, dem erleichtert jQuery die Arbeit. Der einzige Bereich, in dem jQuery erheblich schlechter als andere Frameworks abschneidet, ist die Behandlung von Fehlern: Hier gibt es keine standardisierte Schnittstelle und eine unzureichende Dokumentation.

Fazit

jQuery macht den Umgang mit Javascript einfacher und sicherer, besonders, wenn es um Ajax und DOM-Zugriffe geht. Gestandene Programmierer fühlen sich mit dem gut strukturierten Framework schnell wohl. Es bleibt abzuwarten, wie sich der Framework-„Markt“ in den nächsten Jahren entwickelt. (hb)

MARKUS FRANZ

ist Chief Technology Officer der BF Blogform Search GmbH, Berlin.

iX-Wertung

⊕ nur 30 KByte Umfang
⊕ gute Dokumentation
⊕ einfache Ajax- und XML/DOM-Programmierung
⊖ unausgereifte Fehlerbehandlung



Archivsysteme – Recht und Technik

Aus den Augen

Ulrike Rieß

Nicht zuletzt dank immer neuer gesetzlicher Vorschriften im In- und Ausland muss sich der IT-Verantwortliche verstärkt mit dem Thema „digitale Archivierung“ auseinandersetzen. Da sich nicht jede Lösung für jeden Zweck eignet, gilt es dabei auch, die technische Seite zu betrachten.

Branchenfremde Vorschriften bestimmen zunehmend den Alltagsbetrieb in der Datenverarbeitung. Viele Dateien dürfen nicht mehr gelöscht, sondern müssen für einen bestimmten Zeitraum unveränderlich aufbewahrt werden. Daher rückt das Archiv aus seiner angestaubten dunklen Kemenate ins Zentrum der Datenhaltung. Nicht nur ISO-Prüfer und Rechtsanwälte nutzen seine Eigenschaften, es ist nunmehr hochoffiziell eine Stufe des „Tiered Storage“ und fügt sich damit ins vielbeschworene Information Lifecycle Management (ILM) ein.

Viele Anwender betrachten das Archiv als eine Art langfristiges Backup. Allerdings haben beide Speicherkategorien nichts miteinander zu tun – sieht man davon ab, dass sie die gleichen Medien nutzen. Das Backup dient zur Wiederherstellung einzelner Dateien oder Datenbankinhalte bis hin zu ganzen Laufwerksinhalten oder Datenbanken. Es soll den Betrieb aufrechterhalten und Fehlern von Nutzern und Anwendungen entgegenwirken. Dazu sichert man periodisch – täglich, wöchentlich oder monatlich – den aktuellen Inhalt von Dateisystemen oder Datenbanken, sodass sich im Falle eines Systemcrashs oder Datenverlusts der aktuelle Stand wiederherstellen lässt. Mit fortschreitendem Alter verlieren Sicherungskopien jedoch schnell an Wert.

Ein Backup ist noch kein Archiv

Im Archiv hingegen lagern nicht mehr für den Tagesbetrieb benötigte Dateien, die ein Unternehmen jedoch für eventuell notwendige Prüfungen durch Behörden oder andere Institutionen vorhalten muss. Dokumente, deren Inhalt niemand mehr verändern darf oder soll – etwa Verträge, Versicherungspolicen oder Grundbucheinträge –, legt man sofort in einem Archivsystem ab. Dort sind sie durch Zugriffssperren, eine WORM-Funktion (Write Once Read Many) oder kryptografische Verfahren vor unberechtigtem Zugriff, Veränderung sowie – bis zum Ablauf der Aufbewahrungsfrist – absichtlichem oder unabsichtlichem Löschen geschützt.

In Deutschland verpflichtet das Handelsgesetzbuch Kaufleute zur Aufbewahrung von Geschäftsunterlagen (§ 257 HGB). Ebenso haben alle Unternehmen der gewerblichen Wirtschaft aus steuerlichen Gründen die Aufbewahrungsvorschriften nach § 147 Abgabenordnung (AO) zu erfüllen. Aus denselben Gründen sind sämtliche Geschäfts- und sonstigen Unterlagen aufzubewahren, die für die Besteuerung von Bedeutung sind. Letztlich geht es also um fast jede geschäftliche E-Mail und jedes versandte oder erhaltene elektronische Dokument, unabhängig von Form und Format. Dagegen ist eine Aufbewahrung im Original nur in Ausnahmefällen vorgeschrieben, etwa für Eröffnungsbilanzen, Jahresabschlüsse und die Konzernabschlüsse. Nach Steuerrecht (§ 146 Abs. 2 AO) ist das aufbewahrungspflichtige Schriftgut innerhalb der Bundesrepublik Deutschland aufzubewahren. Das gilt auch für elektronische Archive. Das Handelsgesetzbuch schreibt keinen Ort vor, die

Unterlagen sind jedoch innerhalb einer „angemessenen Frist“ vorzulegen.

Nach Steuerrecht gilt eine Aufbewahrungsfrist von zehn Jahren für Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen und Buchungsbelege. Eine Frist von sechs Jahren gilt für empfangene Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, „soweit sie für die Besteuerung von Bedeutung sind“ – einschließlich E-Mails und anderer elektronischer Dokumente.

Unterschiedlich lange Fristen

Ist die Festsetzungsfrist noch nicht abgelaufen, können sich die Aufbewahrungsfristen verlängern. Grund kann eine begonnene Außenprüfung, die vorläufige Steuerfestsetzung nach § 165 AO, anhängige steuerstraf- oder bußgeldrechtliche Ermittlungen, ein schwebendes oder aufgrund einer Außenprüfung zu erwartendes Rechtsbehelfsverfahren oder die Begründung von Anträgen des Steuerpflichtigen sein. Generell beginnt die Aufbewahrungsfrist mit dem Abschluss des jeweiligen Kalenderjahres; bei Verträgen mit dem Ende des Jahres, in dem der Vertrag endet.

Besonderes Feingefühl verlangt das Archivieren von E-Mails. Nach § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) begeht derjenige eine Straftat, der eine dem Unternehmen zur Übermittlung anvertraute Sendung öffnet oder unterdrückt. Der Administrator darf demnach elektronische Nachrichten nicht filtern, löschen oder öffnen: Nach einem Urteil des OLG Karlsruhe (Az. 1Ws 152/04 vom 10. Januar 2005) erfüllt das Ausfiltern oder Löschen von E-Mails das Tatbestandsmerkmal des „Unterdrückens“ im Sinne des § 206 StGB. Folglich müssen alle elektronischen Nachrichten ins Archiv wandern – einschließlich Spam.

Es existieren insgesamt rund 16 000 andere Gesetze und Vorschriften, die diesen Bereich betreffen. Dazu gehören unter anderem die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Basel II sowie in den USA der Sarbanes-Oxley Act (SOX), die SEC Rule 17a-4, die FDA-Richtlinie 21CFR11 oder die vom US-Verteidigungsministerium (DoD) spezifizierten Kriterien für die Entwicklung von Electronic Records Management Software (5015.2-STD).

Policies als Gesetzeshüter

Um die zahlreichen und oft verwirrenden Gesetzesvorgaben und andere Richtlinien einzuhalten, bemühen sich Hersteller, ihre Archivlösungen mit flexibler Software auszustatten. Für die Unantastbarkeit und somit Unveränderbarkeit der Dateien sorgen Zugriffs- und Autorisierungsprogramme, die nur den verantwortlichen Gruppen oder Personen den Abruf einzelner Dateien erlauben. In dem Zusammenhang spielt das Reporting eine wichtige Rolle: Mit seiner Hilfe lässt sich feststellen, welche Nutzer Zugriff auf welche Informationsbereiche hatten.

Darüber hinaus kann der Administrator sogenannte Policies definieren, die zum Beispiel den Lebenszyklus einer Datei bestimmen. Mit dem mehr oder weniger umfangreichen Regelwerk kann der IT-Verantwortliche festlegen, nach welcher Zeitdauer oder bei welchem Zugriffsschwellwert eine archivierte E-Mail vom teuren Primärspeicher auf kostengünstigere Nearline-Festplatten oder ins Bandarchiv wandert. Außerdem lässt sich mit Policies die Verweildauer (retention time) beziehungsweise das Datum der endgültigen Löschung festlegen.

Policies nehmen dem Administrator viel Arbeit ab und reduzieren dadurch das Fehlerrisiko. Allerdings erfordern sie eine oft langwierige Vorbereitung: das Erfassen und Klassifizieren aller zu archivierenden Dateien sowie das Aufstellen geeigneter Regeln. Da dazu eine genaue Kenntnis aller internen und externen Richtlinien notwendig ist, müssen verschiedene Abteilungen eines Unternehmens – Geschäftsführung, EDV und Buchhaltung – eng zusammenarbeiten.

Die Qual der Wahl des Mediums

Lange Zeit galten Jukeboxen mit CDs oder DVDs sowie Bandbibliotheken als optimale Medien für Archive. Der Markt hat sich in den letzten Jahren jedoch verändert. Das Band als preiswertes Medium hat die optischen Lösungen fast vollständig verdrängt. Dafür findet man häufiger Festplatten, vor allem in der preiswerten SATA-Ausführung.

Als Kriterien für die Wahl des Mediums sollten nicht nur Stromkosten, Administrationsaufwand oder Platzfragen gelten. Vielmehr muss der IT-Manager wissen, in welchem Zeitrahmen ihm Archivdaten zur Verfügung stehen müssen. Der Gesetzgeber macht keine Vorgaben bezüglich des Mediums.

Die Nutzung von CD-R und DVD-R als Medium für Archivsysteme verringert sich. Haben sich die Medien über Jahre und Jahrzehnte als zuverlässige und preiswerte Lösung etabliert, hat der Anwender jedoch immer mit der mechanischen Natur der Wechsler und damit hohen Zugriffszeiten zu kämpfen. Hinzu kommt, dass kaum ein Hersteller eine zuverlässige Aussage zu treffen vermag, wie lange sich Daten zuverlässig auf DVD-R-Medien speichern lassen, bis man sie zwangsweise auf einen neuen Datenträger verlegen muss. In einem Arbeitsbereich mit einer Verweildauer von bis zu 100 Jahren ist das eine unbefriedigende Lösung.

Auf der anderen Seite ist die Jukebox die günstigste Wahl, wenn es um Energieverbrauch, Stellfläche und Wärmeabgabe geht. Die Laufwerke benötigen wesentlich weniger Strom als diejenigen für Bänder, laufen im Gegensatz zu den meisten Festplatten nur, wenn man sie benötigt, und geben dabei kaum Wärme ab. Durch die sehr flachen

iX-TRACT

- Bei der Archivierung von Dateien und Dokumenten sind viele gesetzliche Vorschriften und Richtlinien zu beachten.
- Archivsysteme erleichtern dem IT-Leiter die Arbeit unter anderem mit Policy-Systemen. Eine sorgfältige Planung bleibt jedoch obligatorisch.
- In gängigen Archivsystemen kommen immer häufiger Festplatten als Speichermedium zum Einsatz; optische Medien hingegen werden seltener.

Archivsysteme

Produkt	Revolution 300A	Centera	T2.2+/T4.4+	Hitachi Content Archive Platform (HCAP)	Integrated Archive Platform
Hersteller	Copan Systems	EMC	Gingcom GmbH	Hitachi Data Systems	Hewlett-Packard
Hersteller-URL	www.copansystems.com	germany.emc.com	www.gingcom.com	www.hds.de	www.hp.com
Anbieter	HMK Computer Technologies GmbH	EMC	über autorisierte Händler	diverse	Hewlett-Packard
Anbieter-URL	www.hmk.de	germany.emc.com	www.gingcom.com	www.hds.de	www.hp.com
Bauform/Größe	Rack; 0,76 × 1,22 × 2,21 m³	19" Rack (Standard EIA RS 310)	19" Rack, 11 und 9 U	19" Rack	42 U Rack (Base System), 42 U (Expansion Rack)
Speichermedium	SATA-Festplatten (MAID)	Disk	Tiered Storage (Festplatte/Band); SAS, SATA, LTO-3	Festplatte	Festplatte, RAID-6
Medienkapazität	250/500/750/1000 GByte	1 TByte	400 GByte (Band)	beliebiges Speichersystem von HDS nutzbar	k. A.
Anzahl Medien/Slots	maximal 896	16 – 128 Platten pro Cabinet	24	beliebiges Speichersystem von HDS nutzbar	k. A.
Anzahl Laufwerke	–	–	2 × LTO-3, voll redundant	–	–
Gesamtkapazität	13,5 – 600 TByte (native)	16 – 128 TByte (brutto) pro Cabinet	2,2 – 4,4 TByte nutzbare Kapazität	bis zu 20 PByte	2,1 – 400 TByte
Anzahl Dateien/Objekte	1,5 Mrd.	unbegrenzt	k. A.	bis zu 32 Mrd. Objekte	unbegrenzt
maximale Dateigröße	2,2 TByte	unbegrenzt	k. A.	25 GByte über NFS (Limitierung von NFS), sonst 100 GByte	1,6 GByte
Haltbarkeit der Medien	MTBF 4000 000 h	k. A.	k. A.	k. A.	k. A.
zusätzlicher Plattenspeicher	–	–	✓	–	–
Schnittstellen	1 – 8 × 4 GBit/s FC, iSCSI	100/1000BaseT Ethernet	10/100/1000BaseT Ethernet (redundant)	k. A.	Gigabit Ethernet
Schreibzugriff	Tape Emulation (VTL), NFS v2/v3, CIFS, Copan API	via API	durch Agenten	NFS, CIFS, WebDAV, HTTP(S)	API, CIFS/NFS über Gateway
Lesezugriff	Tape Emulation (VTL), NFS v2/v3, CIFS, Copan API	via API	per Web-GUI	NFS, CIFS, WebDAV, HTTP(S)	API, CIFS/NFS über Gateway
Suchfunktion	benutzerdefinierte Tags	–	Volltextsuche	Volltext-Indexierung und -Suche (optional)	Volltext (unterstützt MS Office, PDF, Text, Zip, XML, E-Mail)
WORM	✓	✓	✓	✓ (WORM-Dateisystem)	✓ (Software)
Verschlüsselung	✓	–	–	✓	✓
Deduplizierung	out of band, blockbasiert	dateibasiert	dateibasiert (Single Instancing)	✓	✓
Content Addressable (CAS)	–	✓	– (nur intern)	✓	✓
Compliance	alle gängigen Vorschriften	✓	GDPdU, GoBS, Basel II, Sarbanes-Oxley Act	§§ 238 ff. HGB, §§ 146, 147 AO, GoB, GoBS, GDPdU u. a.	FRCP 37(b), Sarbanes-Oxley Act, SEC 17a-4, §§ 238, 239 und 257 HGB, §§146, 147 AO, GoB, GoBS, GDPdU
Management	webgestützt	Centera Viewer (CLI)	Web-GUI	Fernwartung; Hitachi Management Suite	separates Admin-Interface
Software	–	Centrastar	–	Management-Software	IAP v2.0
unterstützte Anwendungen	Quantum AMASS, Filetek Storhouse, MS Removable Storage Manager, SGI InfiniteStorage Data Migration Facility, Sun SAM-FS, Veritas Enterprise Vault	alle, die die Centera API beherrschen	Exchange 2000/2003	k.A.	Datei-, E-Mail- und Datenbank-Archivierungssoftware
unterstützte Betriebssysteme	Unix/Linux, Windows; z/OS via LUMINEX Gateway	alle	Windows ab 2000/XP Professional	Unix, Windows	alle
Stromversorgung	redundant; 200 – 240 V/30 A dreiphasig oder 200 – 240 V/40 A einphasig	220 V	redundante Netzteile für jede Komponente		220 – 240 V
Stromverbrauch (Leerlauf)	685 – 2974 W je nach Ausbau	8800 VA pro Cabinet	k. A.	k. A.	3400 VA
Stromverbrauch (Maximum)	1313 – 6495 W je nach Ausbau	8800 VA pro Cabinet	1500 VA	k. A.	9400 VA
besondere Funktionen	Power Managed RAID, Disk Aerobics	Fixed Content Storage, Mirroring	integrierte USV	Custom Metadata, wählbare Hash-Algorithmen, applikationsübergreifende Volltextsuche	Grid-Architektur, Kapazität und Performance unabhängig skalierbar, Remote Replication
Preis	ab 50 000 €	ab 30 000 €	ab 39 800 €	ab 30 000 €	ab 49 000 €

DR550 Modell DR1/DR2	JVC WORM Appliance	Assureon SA	Enterprise Active Archive	Sun StorageTek 5800 System
IBM	JVC	Nexsan	Plasmon	Sun Storagetek
www.ibm.com	www.jvc-pro.de	www.nexsan.com	www.plasmon.com	www.sun.com
IBM	INCOM Storage GmbH	Nexsan	INCOM Storage GmbH	Sun
www.ibm.com	www.incom.eu	www.nexsan.com	www.incom.eu	www.sun.com
25 U (DR1)/1 – 2 36 U Racks (DR2)	Rack	7 U	Rack	Rack
Festplatten (1 TByte SATA, RAID 5/6), optional WORM Tape (LTO, TS1120/TS1130, Sun STK ACLS oder LibraryStations) oder optische WORM-Medien (UDO-2, Sony Blue Laser)	Blu-ray Disc	Festplatte (RAID 6)	optisch (UDO-2)	Festplatten (SATA)
Bänder: LTO-4 800 GByte, TS1130 1 TByte; UDO-2: 60 GByte; Sony Blue Laser: 23 GByte	50 GByte	k. A.	60 GByte	500 GByte
max. 48 Festplatten (DR1), 224 Festplatten (DR2)	50 – 600	k. A.	32 – 1276	32 – 128
bis zu 192 LTO-4 oder TS1130 Laufwerke in einer IBM TS3500 Library, bis zu 8 optische Laufwerke pro Library	1 – 6	k. A.	1 – 12	–
Festplatte: 0,88 – 48,88 TByte roh (DR1)/8 – 224 TByte roh (DR2); bei Migration auf Band über ein PByte	2,5 – 30 TByte	k. A.	0,96 – 76 TByte	16 – 64 TByte
300 – 500 Mio.	unbegrenzt	20 Mio.	unbegrenzt	praktisch unbegrenzt (128 Bit Architektur)
nahezu unbegrenzt	50 GByte	k. A.	60 GByte	praktisch unbegrenzt (128 Bit Architektur)
Platten: 3 – 5 Jahre, Bänder: bis 20 Jahre. Empfohlene Migrationszyklen: alle 3 – 5 Jahre für Platten, alle 5 – 7 Jahre für Bänder	50 Jahre	k. A.	50 Jahre	k. A.
–	0,5 – 30 TByte Cache	–	160 – 2000 GByte	–
1 – 6 × Gigabit Ethernet Ports (Kupfer oder Glasfaser)	2 × Gigabit Ethernet; optional FC	k. A.	2 × Gigabit Ethernet, optional FC	8 – 32 × 1000BaseT Ethernet
TSM API, NFS/CIFS mit optionalem File System Gateway	NFS, CIFS	NAS	NFS, CIFS	Java- und C-APIs
TSM API, NFS/CIFS mit optionalem File System Gateway	NFS, CIFS	NAS	NFS, CIFS	Java- und C-APIs
–	Metadaten-/Volltextsuche optional	✓	Metadaten-/Volltextsuche optional	Integrierte Metadata Query Engine
✓	✓ (physikalisch)	k. A.	✓ (physikalisch)	✓
128 Bit AES, 56 Bit DES (TSM API), AES-256 (Tape Encryption)	optional	256 Bit AES	optional	–
–	optional	dateibasiert (Single Instancing)	optional	–
–	optional	✓ (MD5 + SHA-1 Hash)	optional	✓
✓	alle Vorgaben, die WORM-Ablage der Daten verlangen (GDPdU, AO etc.)	k. A.	GDPdU, AO u. a.	k. A.
integrierte Konsole und Management-Software	Web-GUI	k. A.	Web-GUI	GUI- oder CLI-basiert; E-Mail Alerts
System Storage Archive Manager for AIX	k. A.	k. A.	k. A.	Software Developer Kit (SDK)
siehe www-03.ibm.com/systems/storage/disk/dr/interop.html	alle	k. A.	alle	k. A.
i5OS and OS/400, AIX, HP-UX, Solaris, Linux, Unix System Services for OS/390, Novell Netware	Linux, Unix, OS X, Windows	k. A.	Linux, Unix, Windows	Linux (RHEL4-U4), Solaris 9/10, Windows Server 2003 R2 32 Bit, Windows XP
1 Power Distribution Unit 220 V/15 A) für DR1, 1-4 für DR2	redundante Netzteile	k. A.	Netzteile redundant ab 238 Slots	200 – 240 V einphasig
2400 W (DR1)/5500 W (DR2)	175 – 750 W abhängig von der Cache-Größe	k. A.	275 W	k. A.
2500 W (DR1)/6200 W (DR2)	750 W	k. A.	707 W	k. A.
automatische Verlagerung von Daten auf andere Medien; Backup aller Daten auch auf Band; Zerstörung (Shredding) von Daten; Datenspiegelung zwischen zwei DR550 Sytemen; Hochverfügbarkeitsoption mit redundanten Komponenten	optional Clustercache, Systemspiegelung	k. A.	optional Barcode	Erweiterung auf Multi-Cell-Konfiguration möglich
ab 29 000 €	auf Anfrage	k. A.	auf Anfrage	ab 83 000 €

Medien sind die Gehäuse optischer Libraries vergleichsweise kompakt.

Lebensdauer nach unten korrigiert

Beschreibbare CDs (CD-R, CD-RW) gibt es seit Mitte der 1990er Jahre, ursprünglich mit einer Kapazität von 650 MByte. Die meisten heute erhältlichen Medien fassen 700 MByte. Während alle neuen Laufwerke mit diesen Medien umgehen können, könnten sie ältere Modelle allerdings beschädigen. Gaben die Hersteller die Lebensdauer einer CD ursprünglich mit „unbegrenzt“ an, so hat sich diese Angabe inzwischen auf „unter 10 Jahre“ relativiert.

Als Nachfolger der CD etablierte sich 2002–2003 die beschreibbare DVD (Digital Versatile Disc). Während die Größe der Scheiben gleichblieb, erhöhte sich ihre Kapazität auf 4,7 GByte. Auch für die DVD mussten die Hersteller die Lebenserwartung der Medien immer weiter heruntersetzen – momentan liegen die Angaben im Schnitt bei 10 bis 15 Jahren.

In absehbarerer Zukunft dürfte die Blu-ray Disc einen festen Platz im Archivmarkt erobern. Die ein- oder zweilagigen Medien speichern 25 beziehungsweise 50 GByte. Hersteller TDK präsentierte bereits 2006 einen Prototyp mit sechs Lagen und einer Kapazität von 200 GByte. Pioneer legte erst kürzlich nach und kommt mit 16 Lagen auf 400 GByte. Marktreif sind die High-Capacity-Medien allerdings noch nicht. Verlässliche Angaben zur Haltbarkeit von Blu-ray-Medien gibt es leider ebenfalls noch nicht.

Magneto Optical Disks (MO) sind im Gegensatz zu CDs oder DVDs licht- und temperaturunempfindlich und können daher Daten wesentlich länger zuverlässig speichern. MO-Standardmedien haben einen Durchmesser von 13 cm und speichern bis zu 16,7 GByte, die kleineren Exemplare bringen 2,3 GByte auf einer Scheibe mit 9 cm Durchmesser unter.

MO-Produkte werden nicht mehr aktiv vermarktet, man findet sie jedoch immer noch in vorhandenen Libraries. Als Nachfolger hat sich UDO (Ultra Density Optical) etabliert. Die aktuelle zweite Generation des Formats speichert 60 GByte auf einer zweiseitigen (Wende-)Kassette. Die gegenwärtige Roadmap endet bei 240 GByte Kapazität. Hersteller Plasmon gibt eine Lebenszeit von 50 Jahren für die Phase-Change-Medien an, die in drei Ausführungen zu haben sind: „True Write Once“ für einmaliges Beschreiben sowie Löschschutz, „Compliant Write Once“ mit Löschfunktion und „Rewritable“ als Standardmedium für bis zu 10 000 Schreibzyklen.

Dokumente auf der Rolle

Bänder sind heute die Standardmedien für Archivsysteme. Sie bieten den besten Kompromiss aus Kapazität, Leistung und Kosten. Durch widerstandsfähige Kassetten sind die Medien wesentlich länger haltbar als die optischen – MO und UDO einmal ausgenommen – und auch nicht wie diese äußeren Einflüssen ausgesetzt. Den bei magnetischen Datenträgern prinzipiell fehlenden Schutz vor Löschen und Überschreiben emulieren die meisten Hersteller mithilfe der Laufwerks-Firmware und speziell kodierter WORM-Bandkassetten.

Hinsichtlich des Energieverbrauchs, der Stellfläche und der Wärmeabgabe liegen Bandlösungen im Mittelfeld. Die Laufwerke sind zwar nur aktiv, wenn man ein Band einlegt und Daten liest oder schreibt. Jedoch nimmt die robustere Hardware währenddessen wesentlich mehr Leistung auf. Auch der Transport der Bänder schlägt hier zu Buche. Durch die größeren Medien und die Mechanik vergrößert sich außerdem die benötigte Standfläche für Bandbibliotheken. Hohe Speicherdichten erreichen vor allem die kleineren Autoloader. Deren Kapazität ist allerdings auf einige zig Terabyte begrenzt.

Archive verwenden überwiegend Bänder im robusten einspuligen Halbzoll-Format. Das Digital Linear Tape (DLT) wurde 1984 von DEC eingeführt und bietet in seiner aktuellen Version DLT-S-4 eine Kapazität von 800 GByte bei einem Schreib- und Lesetempo von 60 MByte/s. Allerdings hat der heutige Besitzer Quantum bereits durchblicken lassen, dass die Entwicklung damit beendet ist und man sich stattdessen auf das mit dem Erwerb von Certance (ehemals Seagate) eingekaufte LTO-Format konzentrieren will, das in der Mehrzahl der heute verkauften Bandbibliotheken zu finden ist.

LTO (Linear Tape Open) speichert in der aktuellen vierten Generation 800 GByte auf einem Band und liest und schreibt mit 120 MByte/s. Die einspuligen Kassetten enthalten darüber hinaus einen drahtlos lesbaren Speicherchip (Remote Memory In Cassette, R-MIC), der sowohl den Ladevorgang beschleunigt, als auch das Medien-Management in Bibliotheken vereinfachen kann. Laut Angaben der Hersteller verliert ein Band innerhalb von 20 Jahren durchschnittlich nur 4 % seiner Magnetisierung.

Sonys Advanced Intelligent Tape (AIT) entstand 1996 als Konkurrenz zu DAT/DDS. Das 2006 eingeführte AIT-5-Laufwerk speichert 400 GByte mit 24 MByte/s auf ein 8 mm breites Band in einer kompakten zweispuligen Kassette. Im Gegensatz zu DLT und LTO zeichnet AIT die Daten wie ein Videorekorder schräg auf (Helical Scan Recording). Das erlaubt eine erheblich geringere Laufgeschwindigkeit, was wiederum die mechanische Belastung des Bandes reduziert. Nach demselben Verfahren arbeitet auch SAIT (Super-AIT), allerdings mit Halbzoll-Bandkassetten, deren Bauform mit der von LTO identisch ist. Ein SAIT-2-Streamer bringt darauf 800 GByte unter; mit 45 MByte/s liest und schreibt er jedoch deutlich langsamer als ein LTO-Gerät. Die Laufwerke vertreibt Sony nur mit seinen Petasite-Bibliotheken, ihre Verbreitung ist daher eher gering.

Vornehmlich in Rechenzentren findet man proprietäre Technik wie IBMs 3592-Bandlaufwerke (Codename „Jaguar“) oder die Laufwerksfamilien T9840 und T10000 von Sun Storagetek. Während das aktuelle T9840D mit seinen zweispuligen 75-GByte-Kassetten in erster Linie auf niedrige Zugriffszeiten optimiert ist, bieten IBMs TS1130 und Suns T10000.B bei einem hohen Schreib- und Lesetempo von 160 beziehungsweise 120 MByte/s je ein Terabyte Kapazität pro Band.

Üblicherweise können Bandlaufwerke die von ihren Vorgängern geschriebenen Bänder lesen, meist bis zur jeweils vorletzten Generation. Das erleichtert die Migration der Daten auf neue Medien erheblich.

Daten fahren Karussell

Mit immer höherer Kapazität und gleichzeitig fallenden Preisen werden Festplatten als Speichermedium im Archivbereich attraktiver. Aktuelle SATA-Modelle fassen 1 TByte und erreichen ein Übertragungstempo jenseits der 100 MByte/s. Für August hat Seagate das erste Modell mit einer Kapazität von 1,5 TByte angekündigt.

Zwar gehen Festplatten damit ungefähr pari mit den modernsten Bandsys-

temen. Allerdings benötigen sie erheblich mehr Energie und produzieren mehr Wärme, da die Platten permanent rotieren – auch wenn keine Zugriffe stattfinden. Da man keinen Transportmechanismus benötigt, ist andererseits die Packungsdichte höher als etwa bei einer Tape Library.

Im Gegensatz zu anderen Medien lassen sich Festplatten zu einem RAID-Verbund zusammenfassen, der vor dem Ausfall eines oder gar mehrerer Laufwerke schützt. Das ist allerdings auch notwendig, denn bei einer üblichen Verlässlichkeit (Mean Time Between Failures, kurz MTBF) von 1,2 Millionen Stunden beträgt die sogenannte Annual Failure Rate (AFR) 0,73 % – von 137 Festplatten fällt im Schnitt jedes Jahr eine aus. Selbstverständlich gilt die Kalkulation nur unter Idealbedingungen – ausreichende Kühlung, keine Vibration – und bei Einhaltung des vorgegebenen Duty Cycle. Preiswerte Desktop-Festplatten, die nicht für den Dauerbetrieb konstruiert sind, sterben in der Regel vor ihren teuren Verwandten. Generell sollte man nicht mit einer Lebensdauer von über fünf Jahren rechnen.

Einige Hersteller wie Copan Systems oder Nexsan bedienen sich eines Massive Array of Idle Disks (MAID), um den Stromverbrauch ihrer Systeme zu reduzieren. Es versenkt Festplatten in den Schlafmodus oder schaltet sie ganz aus, solange es sie nicht benötigt. Letzteres kann obendrein die Lebensdauer erhöhen. In Copans MAID etwa steht maximal ein Viertel der Platten unter Strom. Um Schwierigkeiten mit Schmiermitteln und der Mechanik entgegenzuwirken, schalten MAID-Systeme die Platten in regelmäßigen Intervallen ein und überprüfen sie auf Fehler.

Mittlerweile ziehen andere Hersteller nach und lassen die Festplatten zumindest langsamer rotieren, um Energie zu sparen. Dennoch lohnen sich Festplattenarchive nur für Anwender, die in kurzer Zeit auf archivierte Informationen zugreifen müssen, etwa Onlinedienste oder Forschungsinstitute. Energiekosten und Verwaltungsaufwand sind derzeit noch zu groß, um ein festplattenbasiertes Archiv flächendeckend einzusetzen. Es existieren jedoch zahlreiche Archivsysteme, die schnelle Festplatten als Zwischenspeicher (Cache) einsetzen.

Holografische Speicher legen Informationen mit extrem hoher Dichte in Kristallen oder Polymeren ab. Im Gegensatz zu herkömmlichen Medien nutzen sie nicht nur die Oberfläche, sondern das gesamte Volumen des Datenträgers zur Aufzeichnung. Bislang haben sie am Markt jedoch keinerlei Bedeutung. Auch macht keiner der Hersteller Angaben zur Haltbarkeit der Medien, was eine Verwendung als Langzeitspeicher ausschließt.

In der Tabelle sind die Archivsysteme der einschlägigen Hersteller aufgeführt. Rein optische oder Bandarchive sind darin nicht zu finden; selbst die optischen Blu-ray- und UDO-Archive von JVC und Plasmon besitzen zumindest ein Festplatten-Array als Cache. Die Mehrzahl der Hersteller setzt auf Festplatten als Speichermedium, oft mit integrierter oder optionaler Bandbibliothek für besonders große Datenmengen.

Eine Reihe von Archiven – etwa Hewlett-Packards Integrated Archive Platform oder die Hitachi Content Archive Platform – ist modular aufgebaut und erlaubt daher eine nachträgliche Erhöhung der Kapazität oder des Datendurchsatzes. Andere lassen sich durch Hinzufügen weiterer Racks den steigenden Anforderungen anpassen. So ersparen sie dem Nutzer eine aufwendige Migration auf ein neues, größeres System.

Fazit

Ein Archivsystem, das alle Wünsche erfüllt, gibt es nicht. Wer keine besonderen Anforderungen hinsichtlich der Zugriffszeiten oder Datentransferraten hat, kann zwischen Bändern, Festplatten und optischen Medien frei wählen. Allerdings sollte man das Archiv nicht als Einzelanwendung, sondern als Bestandteil der gesamten Speicherstrategie betrachten.

Optische Speicher haben hohe Zugriffszeiten und bieten vergleichsweise geringe Kapazität. Bänder bringen auf einem Medium wesentlich mehr Daten unter, außerdem lesen und schreiben sie schneller. Die Bandwechselzeiten hängen stark von der Robotik der Bibliothek und den eingesetzten Laufwerken ab. Bandlaufwerke benötigen mehr Energie als optische, aber erheblich weniger als Festplatten. Die hingegen trumpfen mit niedrigen Zugriffszeiten und hohem Datendurchsatz auf. Neue Techniken wie MAID senken ihren Energiehunger auf erträgliche Werte.

Darüber hinaus muss der IT-Verantwortliche prüfen, welche Daten ins Archiv gehören und welche Vorschriften er zu befolgen hat, was deren Aufbewahrungszeit, Auditfähigkeit und Unveränderbarkeit angeht. Archivieren besteht nicht mehr nur im Ablegen von Aktenordnern. Vielmehr tragen Archive maßgeblich zur Geschäftstüchtigkeit eines Unternehmens bei und sollten dementsprechend konzipiert sein. (mr)

ULRIKE RIEß

ist freie IT-Journalistin mit langjähriger Erfahrung in der Storage- und Netzwerk-Branche.

Anonymisierende Peer-to-Peer-Netze im Überblick

Unerkannt

Nils Durner, Nathan S. Evans, Christian Grothoff

Die selbst in Deutschland wiederholt bekannt gewordenen Bespitzelungen von kritischen Journalisten durch Staatsorgane und das Misstrauen gegenüber Mitarbeitern oder Kollegen haben auch im Unternehmensbereich das Interesse an anonymer Internetnutzung geweckt. Ein Vergleich von Filesharing-Netzen trennt die Spreu vom Weizen.



Privatsphäre ist ein knappes Gut in einer praktisch gläsernen Gesellschaft. Dabei brauchen fast alle den Datenschutz: Unternehmen wollen Informationen über Kunden, Mitarbeiter und Zulieferer vor der Konkurrenz geheim halten, staatliche Institutionen müssen Informationen und Informationsquellen schützen, Bürger brauchen Freiräume zur Ausübung demokratischer Pflichten.

Dieser Artikel stellt einige grundlegende Techniken zum Schutz der eigenen Online-Identität vor und beurteilt verschiedene Peer-to-Peer-Netze, die diese Techniken nutzen und Anonymität gewährleisten wollen. Vorweg ein Wort zur Begriffsdefinition: Anonymität ist die Fähigkeit einer Person, ihre Aktionen von ihrer Identität zu trennen. Dabei müssen ihre Absichten nicht notwendigerweise illegal sein. So werden beispielsweise Wege gesucht, Informationen wie Einbruchsprotokolle in EDV-Systeme auf sicherem Wege Interessierten ohne etwaigen Imageverlust für die Organisation zur Verfügung zu stellen.

Zur Quantifizierung der Anonymität ziehen Wissenschaftler üblicherweise zwei Schlüsselmetriken heran. Die erste ist die Menge der Verdächtigen. Perfekte Anonymität würde bedeuten, dass alle Menschen als Verdächtige infrage kämen. Online kommen nur alle Menschen mit Internetzugriff in Betracht, und je kleiner die Menge ist, desto weniger anonym ist ein Vorgang. Daher können anonymisierende Netze mit wenigen Benutzern eine schlechte Wahl sein.

Die zweite Metrik ist komplizierter. Sie nimmt an, dass basierend auf Beobachtungen der Feind einem jedem Verdächtigen eine Täterwahrscheinlichkeit zuweisen kann. Perfekte Anonymität wäre erreicht, wenn unter n Verdächtigen jeder einzelne eine Täterwahrscheinlichkeit von 1/n zugewiesen bekäme. Die größte Täterwahrscheinlichkeit eines einzelnen Verdächtigen ist dann eine einfache Metrik, mit der man den Grad der gebotenen Anonymität beurteilen kann.

Eine weitere unter Wissenschaftlern beliebte Metrik ist die Entropie der Wahrscheinlichkeitsverteilung. Informationstheoretisch gesehen liefert diese zwar ein schönes Modell, jedoch dürfte in der Praxis die Täterwahrscheinlichkeit wichtiger sein, da Wahrscheinlichkeiten für juristische Urteile von Bedeutung sind.

Naturgemäß sind die Fähigkeiten und Möglichkeiten des Angreifers ent-

scheidend. Ein realistisches Modell für P2P-Filesharing-Netze ist ein aktiver Feind, der genau wie alle anderen am Netz teilnimmt und dem es gestattet ist, Anfragen zu stellen, um weitergehende Informationen zu bekommen.

Der Feind in deinem Netz

Die von den Autoren früher durchgeführten Angriffe auf Freenets Darknet-Routing-Protokoll [2] und Stealthnet [1] fallen in diese Kategorie: Jeder technisch fähige Nutzer mit einer Standard-DSL-Internetverbindung könnte den Quellcode seines Peers verändern, dem P2P-Netz als scheinbar normaler Teilnehmer beitreten und versuchen, es von innen heraus anzugreifen. Die Haupteinschränkungen für einen solchen Angreifer sind, dass seine Rechenkapazitäten begrenzt sind, er im Rahmen des Protokolls handeln muss und nicht die direkte Kommunikation von zwei anderen Knoten untereinander überwachen oder gar kontrollieren kann.

Während sich der Großteil der Forschung auf kleinere Variationen dieses Modells beschränkt, verlangt die Realität darüber hinaus oft nach Lösungen, die auch einem Feind standhalten, der entweder in der Lage ist, selektiv die Kommunikation zwischen normalen Benutzern zu unterbrechen oder gar die Kontrolle über die Maschine des Benutzers hat (zum Beispiel durch Rootkits oder Keylogger). Sobald der Feind in der Lage ist, einzelne Benutzer zu isolieren, um so ihre P2P-Kommunikation auf feindkontrollierte Systeme zu beschränken, wird Anonymität unmöglich: Im resultierenden Netz gibt es nur einen Verdächtigen, daher ist für jede Aktion der Urheber sofort bekannt.

Eine Variante der Kontrollübernahme ist übrigens die Beschlagnahme eines Knotens durch die Sicherheitsbehörden. Die Vorschriften zur Vorratsdatenspeicherung greifen in Deutschland auch bei Anonymisierungsdiensten – aber auch ganz unabhängig von der jeweiligen nationalen Rechtslage kann es vorkommen, dass der betreffende Rechner erst einmal in den Händen der Polizei landet. Darum ist die Frage nicht uninteressant, ob auf diesem Wege eine Deanonymisierung technisch möglich ist.

Eckdaten der Anonymisierungsnetze

Netz	URL	Programmgröße	Sprache	deutsche Übersetzung	Plattformen
Freenet	freenetproject.org	373 KB	Java	teilweise	Java/Any
Entropy	entropy.stop1984.com	861 KB	C	nur online	B/L/O/W
Mute	mute-net.sourceforge.net	708 KB	C/C++	nein	B/L/O/W
Ants	sourceforge.net/projects/antsp2p.net	7,5 MB	Java	nein	Java/Any
Stealthnet	www.Stealthnet.de	450 KB	C#	ja	L/W
Tor	www.torproject.org	1,5 MB	C	nur online	B/L/O/W
Jap	anon.inf.tu-dresden.de	5,6 MB	Java	ja	Java/Any
Mixminion	www.mixminion.net	483 KB	C/Python	nein	B/L/O/W
I2P	www.i2p2.de	9,2 MB	Java	nur online	Java/Any
GNUnet	gnunet.org	2,5 MB	C	teilweise	B/L/O/W

Erste Annäherung: die Eckdaten der Anonymisierungsnetze (B = BSD, L = Linux, O = OS X, W = W32)

Techniken zur Online-Anonymität

Wenn Systeme bidirektionale Kommunikationskanäle über das Internet aufbauen, erfahren beide Endpunkte die IP-Adresse des Partners. Da es praktisch immer möglich ist, diese einer Person oder Institution zuzuordnen, ist keiner der Kommunikationspartner anonym. Werden zur Anonymisierung Systeme zwischengeschaltet, muss jeder Endpunkt nur die IP-Adresse des nächstgelegenen Mittelsmannes kennen, nicht die der Partner selbst. Da jedoch die Kommunikationsteilnehmer nicht unbedingt auf die Ehrlichkeit der Mittelsmänner vertrauen können, ist der Aufbau anonymer Verbindungen in der Praxis etwas komplizierter. Anonyme Netze müssen Systeme verbinden, ohne Endpunkte zu identifizieren, nicht einmal gegenüber den Mittelsmännern.

Um die Verbindung zwischen Aktionen und Person zu verschleiern, sind Indirektion und Mischung, gegebenenfalls in Kombination mit künstlichen Verzögerungen, gängige Schlüsseltechniken. Die meisten Systeme verwenden zusätzliche Verschlüsselung, um Angreifern die Korrelation zwischen Inhalten und Datenfluss zu erschweren. Fast immer wird Verschlüsselung für die direkte Verbindung zwischen zwei Teilnehmern (Link- oder Point-to-Point-Verschlüsselung) verwendet, in manchen Fällen wird zudem zwischen den Kommunikationsendpunkten (End-to-End) verschlüsselt.

In diesem Zusammenhang ist eine Unterscheidung zwischen Absender- und Empfänger-Anonymität nötig. Wird lediglich Absenderanonymität gewünscht, kann der Absender den Mittelsmännern die Identität des Empfängers mitteilen und das Netz einen Kommunikationspfad zu dem bekannten Ziel aufbauen. Wird außerdem Empfängeranonymität benötigt, muss das Netz eine Möglichkeit bereitstellen, den Empfänger ausfindig zu machen. Dies ist schwierig, da ein Feind nicht in der Lage sein darf, denselben Prozess zu nutzen, um die Identität des Empfängers zu ermitteln.

In Filesharing-Netzen sind Benutzer üblicherweise weniger an einem bestimmten Empfänger, sondern eher an einer bestimmten Datei interessiert. Trotzdem ist die Problemstellung ähnlich: einen Pfad zu dem System, das die Datei anbietet, aufbauen, ohne dass ein Widersacher in die Lage versetzt wird, die Identität dieses Systems in Erfahrung zu bringen. Übliche Lösungen für dieses Problem sind entweder die Bereitstellung eines Treffpunktes im Netz, der einen bereits existierenden Kanal zum Zielsystem unterhält, oder die Konstruktion eines (hauptsächlich zufälligen) Pfades durch das Netz, in der Absicht, irgendwann das gewünschte Zielsystem mehr oder weniger durch Glück zu erreichen.

iX-TRACT

- Arbeitsweise und Algorithmen anonymisierender Netze sollten offengelegt und transparent sein, was in der Regel nur freie, quelloffene Software gewährleistet.
- Die Zahl der Teilnehmer ist ein entscheidender Faktor für die Wirksamkeit der Anonymisierung.
- Wer das Internet anonym nutzen will, muss sich mit Performance-Einbußen abfinden.

Verzögerungen und Mischen

Während die Umleitung von Nachrichten über Zwischenstationen es für Mittelsmänner und Endpunkte schwierig macht, die IP-Adresse des anderen

Systems herauszufinden, ist dies für einen Feind, der den gesamten Netzverkehr sehen kann, kein Problem. Der Feind würde das Verkehrsaufkommen, das von einem Teilnehmer ausgeht, mit den Datenmengen vergleichen, die andere Teilnehmer empfangen und im gleichen Zeitraum und Umfang weiterleiten. Das letzte System in einer solchen Kette wäre als Empfänger identifiziert.

Dazu braucht es nicht einmal eine Kenntnis des Inhalts, Verschlüsselung hilft dagegen also nicht. Erst die Kombination von Verschlüsselung mit zufällig gewählten künstlichen Verzögerungen an jeder Zwischenstation macht es für den Feind schwieriger, den Verkehr zeitlich zu korrelieren. Doch: Zu lange Verzögerungen führen zu Beeinträchtigungen bei Anwendungen, von denen Antworten mit geringer Verzögerung erwartet werden, zu kurze machen möglicherweise Korrelationen nicht unmöglich.

Anonymisierende Netze können Flussanalysen durch künstlich erzeugtes Datenrauschen zusätzlich erschweren – wie Wei Dai’s PipeNet [3] –, doch das kostet Bandbreite.

Durch das oft ohnehin stattfindende Mischen von Datenströmen durch NAT-Geräte sind interne IP-Adressen von Nutzern im lokalen Netz für Beobachter im Internet nicht sichtbar. Solange eine genügend große Anzahl an Benutzern das gleiche NAT-Gerät benutzen und der Angreifer keinen Zugriff auf die Operationsdaten des NAT hat, ist eine gewisse Anonymität des Absenders erreicht. Da typische Heim- und Institutionsnetze tatsächlich jedoch einen vergleichsweise engen Benutzerkreis haben, ist die gebotene Anonymität im Allgemeinen nicht ausreichend. Zudem bietet NAT nur Absender-Anonymität, da keine Anfragen anonym empfangen werden können.

Trügerisch: Offene Proxies

Minimale Absender-Anonymität durch Indirektion lässt sich auch durch die Verwendung von offenen, öffentlichen oder bezahlten Proxy-Diensten erreichen. Offene Proxies sind Proxies, die keine Zugriffskontrollen besitzen (in manchen Fällen nur aus Versehen, ähnlich offenen WLANs), was es jedermann erlaubt, ihre Dienste in Anspruch zu nehmen.

Die Verwendung eines einzelnen offenen Proxy ist einfach, ein Proxy-Server lässt sich in den meisten Browsern einstellen. Darüber hinaus macht es die Erweiterung Switchproxy für Firefox einfach, zwischen mehreren Proxies zu wechseln. Doch sind die IP-Adressen beider Kommunikationspartner nicht nur für den Proxy-Betreiber sichtbar, sondern werden in der Regel sogar protokolliert. Und das häufige Fehlen jeglicher Verschlüsselung ermöglicht es dem Betreiber, die Verbindung abzuhören oder sogar Antworten zu fälschen. Weiterhin enthüllen einige Proxies (wie Squid und Apaches *mod_proxy*) die IP-Adresse des Anfragenden standardmäßig als Teil des HTTP-Headers.

Allgemeine Herausforderungen

Eine wesentliche Schwachstelle eines jeden anonymisierenden Netzes ist, dass jede Zwischenstation in bestimmtem Umfang Zustandsinformationen halten muss, um Nachrichten routen zu können. Da das sogenannte „Mischen“ besonders effektiv ist, wenn die Zwischenstation mehrere Datenströme gleichzeitig verarbeitet, ist Zustandsmanagement entscheidend für skalierbare und sichere anonyme Netzanwendungen.

Da Mittelsmännern generell nicht vertraut werden kann, liegt die andere Hauptschwierigkeit darin, gute Zwischenstationen zu finden und auszuwählen. Geht es zusätzlich um Empfängeranonymität, ist das Auffinden eines Ziels, ohne dabei dessen Identiät zu enthüllen, eine weitere Herausforderung. Schlussendlich sind Zwischenstationen, die die Identität von Endpunkten in Erfahrung bringen können, vor Angriffen feindlicher Endpunkte zu schützen.

Die hier vorgestellte Auswahl ist auf freie Software zum anonymen Filesharing und /oder zur anonymen Kommunikation beschränkt. Proprietäre und Closed-Source-Programme sind besonders im Hinblick auf ihre Sicherheit wesentlich schwieriger zu bewerten und daher nicht zu empfehlen.

Die Netze unterscheiden sich stark hinsichtlich Qualität und Dokumentation. Gelegentlich neigen die dahinterstehenden Macher zu vollmundigen Versprechungen, ihre Lösungen seien „völlig“ sicher und anonym. Benutzer sollten vorsichtig sein, insbesondere wenn nur irreführende, ungenaue oder gar keine Dokumentation zur Verfügung steht [1].

Freenet 0.5/0.7 und Entropy

Freenet, nicht zu verwechseln mit der Hamburger Freenet AG, war das erste praktisch genutzte anonyme P2P-Filesharing-Netz und sein Design das Vorbild für viele andere. Es ist in Java geschrieben und ermöglicht, anonym Webseiten zu veröffentlichen, Dateien zu tauschen und online zu kommunizieren. Derzeit sind zwei Versionen in Verwendung: 0.5 und 0.7. Version 0.5 verwendet den ursprünglichen Freenet-Routing-Algorithmus, der 1999 entworfen [4] und aus Skalierbarkeits- und Sicherheitsgründen in Version 0.7 abgelöst wurde. Da die Algorithmen inkompatibel sind, gibt es tatsächlich zwei Freenet-Netze.

Die Hauptmechanismen beider Freenet-Versionen sind die gleichen.

Performance und Sucherfolg

Netz	Netzgröße (Knoten)	Download-Zeit (10 MByte)	Suchergebnisse	Speicherverbrauch	Prozessorlast
Freenet	1000–5000	10 min	N/A	90 MB	<5 %
Entropy	<10	15 min	N/A	24 MB	<1 %
Mute	10–50	4 bis 6 min	1834	4 MB	<5 %
Ants	<10	–	141	50 MB	<1 %
Stealthnet	200–300	2 min 5 s	2097	62 MB	5 %
Tor	>10000	8 min bis 1 h	N/A	13 MB	<1 %
Jap	5–10	10 min 30 s	N/A	62 MB	<3 %
Mixminion	25–30	13 h 20 min	N/A	unbekannt	unbekannt
I2P	100–1000	1 h 15 min	831	27 MB	<1 %
GNUnet	150–200	1 h 14 min	662	26 MB	<5 %

Daten zu den Netzen, die halbwegs objektiv durch Messung ermittelt werden konnten. Die Netzgröße, als Anzahl der Knoten im Netz, beruht entweder auf eigenen Messungen der Autoren (soweit möglich) oder auf Schätzungen der Entwickler der Software (soweit verfügbar). Die angegebene Download-Zeit ist die Zeit für den Transfer einer 10-MByte-Datei zwischen zwei verschiedenen Rechnern im P2P-Netz. Speicherverbrauch und Prozessorlast wurden ohne aktives Suchen oder Downloads unter Windows gemessen.

Wie Anonymität erreicht wird

Netz	Pfadwahl durch	Pfadwahl-Methode	künstliche Verzögerung	Schlüssel-wortsuche	URI/URL-basierter Download	Integritäts-prüfungsebene	Link-Verschlüsselung	End-to-End-Verschlüsselung	verschlüsselte Suche
Freenet	Mittelsmann	Distanz	nein	ja	ja	Datei	ja	ja	ja
Entropy	Mittelsmann	Distanz	nein	ja	ja	Datei	ja	ja	ja
Mute	Mittelsmann	Zufall & Erfahrung	nein	ja	ja	Datei	ja	nein	nein
Ants	Mittelsmann	Zufall & Erfahrung	nein	ja	ja	Datei	ja	ja	nein
Stealthnet	Mittelsmann	Zufall & Erfahrung	nein	ja	nein	Datei	ja	ja	nein
Tor	Sender	Zufall & Ressourcen	nein	nein	ja	Tunnel	ja	ja*	n/a
Jap	Sender	Zufall	nein	nein	ja	Tunnel	ja	ja*	n/a
Mixminion	Sender	Zufall	ja	nein	nein	Tunnel	ja	ja	n/a
I2P	Sender	Zufall	nein	nein	ja	Tunnel	ja	ja	n/a
GNUnet	Mittelsmann	Zufall & Erfahrung & Ressourcen	ja	ja	ja	Block	ja	ja	ja

(*): Daten sind bei Tor und Jap nur dann verschlüsselt, wenn die Anfrage HTTPS oder ein anderes auf Anwendungsebene bereits verschlüsseltes Protokoll benutzt.

Anonymisierungsmethoden der P2P-Netze

Jeder Knoten und jeder gespeicherte Datenblock haben einen eindeutigen Bezeichner. Das 0.7-Netz speichert Daten möglichst auf dem Knoten, dessen Bezeichner dem Bezeichner der Daten am nächsten ist. Werden Daten eingefügt oder gesucht, wird die Anfrage Schritt für Schritt an den Nachbarknoten mit dem zum Datenpaket ähnlichsten Bezeichner weitergeleitet. Die Anonymitätseigenschaften leiten sich aus der inhärenten Indirektion dieses Routing-Protokolls ab. In Freenet cachen Knoten außerdem die letzten gesehenen Inhalte. Das steigert sowohl die Geschwindigkeit als auch die Anonymität, da es dem Feind schwerer gemacht wird, die Quelle der Inhalte festzustellen: Das Anfragen von Inhalten verursacht die Verbreitung dieser Inhalte im Netz.

Während das Routing in 0.7 schneller ist, kann es darüber hinaus die Anonymität eines anfragenden Knotens kompromittieren. Freenet 0.7 begegnet dem mit der Möglichkeit, Verbindungen auf Freunde zu begrenzen und ein Friend-to-Friend-Netz (F2F) zu bilden, in dem nur die verbundenen Freunde von der Teilnahme des Knotens wissen. Die größte Schwachstelle eines F2F-Netzes ist allerdings meist die mangelnde Größe, was kontraproduktiv für den Anonymisierungsgrad ist. Zudem können bösartige Peers DoS-Angriffe auf den Routing-Algorithmus durchführen [2], was zum Datenverlust führen kann.

Entropy, was für „Emerging Network To Reduce Orwellian Potency Yield“ steht, ist eine alternative Realisierung des Freenet-0.5-Protokolls; Entropy verbindet sich mit dem Freenet-0.5-Netz. Ein Designziel war, durch C statt Java schneller zu sein als die ursprüngliche Freenet-0.5-Implementierung. Ansonsten teilt Entropy die Vor- und Nachteile von Freenet 0.5.



Mute und Ants

Mute und Ants verwenden netzspezifische Knotenbezeichner an Stelle von IP-Adressen zum Routing um Anonymität zu erreichen. Peers bekommen durchaus die IP-Adressen von Knoten im Netz mit, sie wissen aber nicht, welche IP-Adresse welchem Knotenbezeichner entspricht. Anfragen und Antworten spezifizieren Knotenbezeichner und nicht IP-Adressen. Die Schlüsselidee hinter den Routing-Algorithmen von Mute und Ants ist, dass Peers über empfangene Nachrichten lernen, welcher ihrer Nachbarn die nächste Station ist, wenn sie selbst Daten zu einem bestimmten Knotenbezeichner routen möchten.

Solange ein Feind den Zusammenhang von IP-Adresse und Knotenbezeichner nicht feststellen kann, wird von dem Protokoll angenommen, dass es Anonymität bietet. Aus Performancegründen schützt das Protokoll nicht vor Angriffen, die auf Zeitmessung und Verkehrsvolumen basieren.

Eine der Herausforderungen in diesem Zusammenhang ist, wie suchende Peers verhindern können, das Netz zu fluten und trotzdem anonym zu bleiben

– immerhin ist bei Suchen das Ziel unbekannt. Außerdem funktionieren traditionelle Internetmechanismen wie das einfache Führen eines Hop Counters (und dem Beenden einer Suche nach n Hops) nicht für anonyme Netze: Ein Hop Counter von 0 würde den Initiator deanonymisieren, eine Antwort mit maximal zulässigem Hop-Count würde den Antwortenden deanonymisieren. Eine Lösung dieses Problems, die Mute, Ants und Stealthnet (und in gewissem Sinne sogar Freenet 0.5) gemeinsam haben, ist, dass bei der Interpretation des Hop Counters der Zufall mitspielt. Dies macht es statistisch gesehen jedem Peer möglich, auf jede Anfrage zu antworten (aber nicht zu wahrscheinlich, um unkontrolliertem Flooding vorzubeugen). Genauso bleibt die Identität des Initiators geheim, indem spezielle Hop-Counter-Werte verwendet werden, die mit gewisser Wahrscheinlichkeit von einem anderen Knoten stammen könnten.

Hauptunterschied zwischen Mute und Ants: Ants ist in Java geschrieben, Mute in C++ und dementsprechend sind die Benutzeroberflächen verschieden. Intern unterscheiden sich Mute und Ants außerdem in kleineren Details des Protokolls. Beispielsweise bietet Ants End-to-End-Verschlüsselung, die sich jedoch leicht durch Man-in-the-Middle-Angriffe umgehen lässt und deshalb in Mute nicht implementiert ist. In der Praxis bietet End-to-End-Verschlüsselung bei geringen zusätzlichen Kosten etwas Schutz gegen Feinde, die sich weniger ausgefeilter Techniken bedienen. Ein weiterer Unterschied ist, dass Ants mit bestimmter Wahrscheinlichkeit Anfragen einfach verwirft, was das Netz weniger konsistent arbeiten lässt, es durch erhöhte Unberechenbarkeit aber auch Feinden etwas schwerer macht.

Popularität und Alter

Netz	Popularität	Projektstart	letzte Release
Freenet	4.91	2000	1/2008
Entropy	0.34	2002	10/2005
Mute	2.52	2004	4/2007
Ants	0.12	2004	1/2007
Stealthnet	n. v.	2006	4/2008
Tor	6.92	2005	1/2008
Jap	1.23	2000	2/2008
Mixminion	n. v.	2002	9/2007
I2P (IIP)	0.73	2002	3/2008
GNUnet	6.52	2001	12/2007

Ungefähre Daten zur Popularität, basierend auf Daten von Freshmeat.net im April 2008. Zu beachten ist, dass aufgrund der verwendeten Rechenmethode ältere Projekte bei gleicher Popularität im Vergleich mit neuen Projekten mehr Popularitätspunkte haben.

Des Weiteren verwendet Ants unter anderem IRC-Kommunikation zum automatischen Aufspüren anderer Peers, was nicht nur für die Einheit des Netzes geschickt ist, sondern nebenbei auch noch einen eingebauten nicht-anonymen Chat-Client mit sich bringt. Darüber hinaus unterstützt Ants Swarming, also die Möglichkeit, von mehreren (möglicherweise unvollständigen) Quellen parallel herunterladen zu können.



Stealthnet

Stealthnet, vormals besser bekannt als RShare, ist ein P2P-Filesharing-Netz, das ziemlich populär in Deutschland, aber relativ unbekannt im Rest der Welt ist. Dementsprechend haben die angebotenen Inhalte eine starke Ausrichtung auf deutsche Medien. Anonymität wird in Stealthnet durch Indirektion erreicht, die Daten durch eine Variante der von Mute und Ants bekannten Algorithmen über andere Peers ohne künstliche Verzögerung geroutet. Einfache Benutzung und hohe Geschwindigkeit sind die Hauptvorteile gegenüber anderen anonymen P2P-Netzen.

Allerdings waren Wissenschaftler in vorherigen Versionen in der Lage, Benutzer des Netzes zu deanonymisieren. Während die Entwickler manche der Schwachstellen behoben haben, bleiben einige Bedenken. Zum Beispiel sendet Stealthnet Anfragen im Klartext, was es bösartigen Peers erlaubt, auf jede Anfrage mit einer großen Anzahl an plausiblen, aber nutzlosen Ergebnissen zu antworten, was das Aufspüren der echten Ergebnisse zur Suche nach der Nadel im Heuhaufen macht. Ebenso könnten arglistige Peers echte Suchergebnisse so verfälschen, dass Peers bei falschen Servern einen Download versuchen oder eine andere Datei – im schlimmsten Fall Malware – bekommen. Dieses Problem besteht übrigens auch in anderen Netzen wie Mute und Ants, von den Folgen können Benutzer populärer Netze wie Gnutella, eDonkey und Kazaa ein Lied singen.

Anders als die Stealthnet-Entwickler behaupten, ist der Schutz vor Denial-of-Service-Angriffen in Stealthnet inadäquat. Die eingesetzten Maßnahmen gegen das Fluten des Netzes sind auf einfache Timeout-Mechanismen beschränkt und verhindern nur, dass im normalen Betrieb Nachrichten für immer zirkulieren. Das Protokoll kann nicht verhindern, dass ein bösartiger Peer eine große Anzahl an Anfragen erzeugt und diese dann im Netz für einen längeren Zeitraum zirkulieren und es so überlasten.



Tor

Tor erreicht die Anonymität für seine Benutzer, indem es als Proxy für TCP-Verbindungen fungiert und eine indirekte Verbindung zum Ziel über das Tor-Netz herstellt. Im Tor-Netz entscheidet der initiierende Peer, welche Tor-Router zur Kommunikation benutzt werden – im Unterschied zur Vorgehensweise von Mute, Ants und Stealthnet, bei denen jeder einzelne Knoten den nächsten Knoten auswählt. Jeder Knoten auf der Strecke (mit Ausnahme des Initiators) weiß nur vom vorhergehenden und dem nachfolgenden Knoten. Der Initiator verschlüsselt seine Kommunikation für jeden Knoten auf der Strecke mit einem unterschiedlichen Schlüssel. Jeder dieser Knoten führt mit jeder empfangenen Nachricht eine Entschlüsselungsoperation durch und leitet das Ergebnis an den nächsten Peer ohne künstliche Verzögerung weiter (Abbildung 1).

Beim Einsatz von Tor als Proxy für unverschlüsselte Protokolle wie HTTP ist zu beachten, dass der letzte Tor-Router Anfrage und Antwort in Klartext sehen kann. Benutzer sollten darum sicherstellen, dass der Datenstrom verschlüsselt ist (wie bei HTTPS), oder keine sensiblen Informationen übertragen.

Da Tor den Absender in die Lage versetzt, eine zufällige Strecke durch das Tor-Netz zu wählen, wird es mit zwei Herausforderungen konfrontiert.

Zum einen ist es schwierig, auf sichere Weise aktuelle Peer-Verzeichnisse zu verteilen. Idealerweise ist jeder Absender in der Lage, eine komplette Liste aller derzeit aktiven Tor-Knoten zu bekommen. Da es einem Feind nicht möglich sein darf, die Verzeichnislisten zu kontrollieren, verwendet Tor mehrere Verzeichnisserver und stellt sicher, dass eine Mehrheit dieser Server bezüglich dieser Verzeichniseinträge übereinstimmt. Das zweite Problem dieser öffentlichen Verzeichnisse ist, dass alle Tor-Router öffentlich bekannt sind und es so für ISPs, Webseiten, staatliche Institutionen, IRC-Netze und andere einfach ist, Anfragen von Tor-Routern zu sperren.

Tor hat eine große Benutzergemeinde und mehr als tausend Router im Einsatz, obwohl deren Betrieb ehrenamtlich ist. Der Betrieb eines Tor-Routers kann außerdem gefährlich sein, da Tor es einem Angreifer gegebenenfalls ermöglicht, Firewalls zu umgehen und Systeme anzugreifen und es dabei so aussehen lassen kann, als ginge der Angriff vom Betreiber des Tor-Routers aus.



JAP

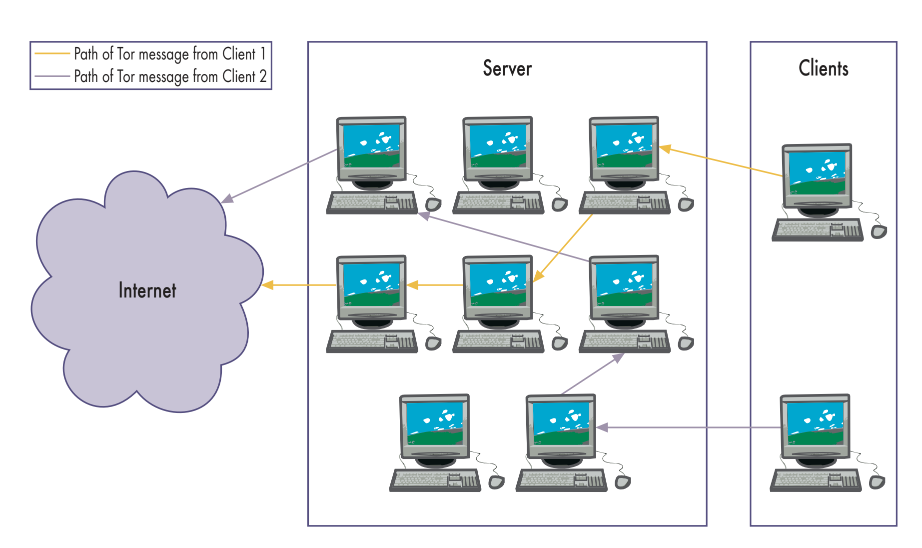
JAPs Design ähnelt stark dem von Tor. Die Hauptunterschiede sind, dass Tor in C implementiert ist, in großem Umfang verwendet und international entwickelt wird. JAP hingegen ist in Java implementiert sowie hauptsächlich in Deutschland entwickelt und verwendet. Die kleinere Benutzergemeinde und die beschränkte geografische Verteilung der Benutzer, Entwickler und Proxy-Betreiber sind problematisch in Bezug auf die Anonymität von JAP-Benutzern im Vergleich zu Tor-Usern. Als C-Anwendung benötigt Tor außerdem weniger Ressourcen. Andererseits bietet Java zusätzliche Sicherheitsvorkehrungen auf Programmiersprachen-Ebene.

Von JAP existieren eine kostenlose und eine kostenpflichtige Variante. Letztere kann zwar mit höherer Performance aufwarten, die Anonymisierung ist aber wegen der geringeren Teilnehmerzahl und der Autorisierungsanforderung schlechter.



Mixminion

Mixminion [5] enthält ebenfalls einige Aspekte von Tor, wie die Verwendung von Verzeichnisservern und das Mischen. Doch im Unterschied zu Tor handelt es sich bei Mixminion um ein Hochlatenz-Netz: Zur Verbesserung der Anonymität verzögern die Peers Anfragen recht lange, ein paar Stunden Verzögerung dürfen für den Benutzer keine Rolle spielen. Hintergrund: Mixminion ist vor allem für E-Mail gedacht, wo hohe Latenzen tolerierbar sind. Mixminion ist der Nachfahre von Mixmaster [6] und verbessert dessen Sicherheit unter verschiedenen Gesichtspunkten. Hervorzuheben ist, dass Mixminion es dem Empfänger erlaubt, auf eine E-Mail eines anonymen Absenders zu antworten, ohne dessen Anonymität zu brechen. Mixminions Design ist vermutlich das sicherste in Bezug auf Anonymität.



Routing bei Tor: Jeder Client entscheidet über den Weg durch das Netz (Abb. 1).



I2P

I2P, früher unter dem Namen „Invisible Internet Project (IIP)“ bekannt, ist eine anonymisierende Netzwerkschicht, die eine sichere und anonyme Kommunikation zwischen Knoten im Netz ermöglicht. Genau wie Tor und JAP verwendet I2P vom Absender aufgebaute verschlüsselte Tunnel, um Daten zwischen den Knoten zu übertragen. I2P bietet sowohl Point-to-Point als auch End-to-End-Verschlüsselung,

I2P hat sein eigenes Netz anonymer Websites („Eepsites“), die ausschließlich im I2P-Netz gehostet und zur Verfügung gestellt werden. Neben Filesharing sind beliebte Anwendungen von I2P anonyme Blogs, Newsgroups und Foren mit Syndie. Die Gnutella-Variante I2Phex verwendet das I2P-Framework zur Anonymisierung dieses traditionellen Filesharing-Protokolls.



GNUnet

GNUnet ist, wie I2P, ein Framework für die Konstruktion sicherer P2P-Anwendungen. Es bietet Funktionen wie das Auffinden anderer Knoten, Point-to-Point-Verschlüsselung von P2P-Kommunikation über TCP, UDP, HTTP und SMTP und eine Ressourcenzuteilung, die sich an der Leistung beziehungsweise den Verdiensten orientiert, die der Knoten durch sein Verhalten in der Vergangenheit erworben hat.

Die bislang einzige für Endbenutzer nützliche Anwendung ist anonymes und zensurresistentes Filesharing; Chat und Newsgroups sind derzeit noch in der Planungs- respektive Entwicklungsphase. Die Filesharing-Anwendung beinhaltet eine Reihe spezieller Features, zum Beispiel die Extraktion von Metadaten aus Dateien unter der Verwendung von GNU *libextractor*, Downloads von mehreren Quellen (Swarming), Veröffentlichung unter gesicherten Pseudonymen, Dateisammlungen (tatsächliche oder virtuelle Verzeichnisse) und den Schutz vor von Mittelsmännern ge- oder verfälschten Suchergebnissen oder Downloads.

Die grundlegende Idee hinter GNUnets Algorithmus zum anonymen Routing ist, dass Peers nicht ihre Anonymität erreichen sollen, indem sie durch Indirektion Ressourcen anderer Peers ausbeuten, sondern ihren eigenen Verkehr mit dem Verkehr, den sie für andere weiterleiten, vermengen. Anonymität gilt als erreicht, wenn ein Feind nicht unterscheiden kann, ob Verkehr von einem Peer stammt oder auf Geheiß anderer weitergeleitet wird.

Anders als bei anderen Netzen dürfen sich Peers auch dazu entscheiden, ihren Verkehr nicht perfekt mit fremdem Verkehr zu vermengen, was ihre eigene Geschwindigkeit verbessert – und ihre eigene Anonymität beeinträchtigt. Dies erlaubt es den Knoten, ökonomische Entscheidungen in Bezug auf das Routing zu treffen: Benutzer können für jede einzelne Aktion den Grad der gewünschten Anonymität festlegen – ohne dabei die Anonymität anderer Benutzer zu kompromittieren.

Der Haupt-Download von GNUnet umfasst nur in der Windows-Version neben den Kommandozeilen-Werkzeugen eine grafische Oberfläche. Für andere Plattformen muss die GTK+ beziehungsweise Qt-basierte Benutzeroberfläche separat heruntergeladen werden. Problematisch ist, dass GNUnet-Protokolle wiederholt nicht rückwärtskompatibel waren und das im jüngst veröffentlichten 0.8.0 Release wieder der Fall ist. Infolge dieser Kompatibilitätsprobleme ist der Benutzerkreis innerhalb eines kompatiblen Netzes möglicherweise zu klein, um

Benutzern ausreichende Anonymität vor starken Feinden zu bieten.

Neben den hier aufgeführten existieren weitere P2P Netze. Aber diese sind durch abweichende Zielsetzungen (WASTE, Retroshare, UseNeXT) oder grundlegende Mängel (OFF System, Omemo, Nodezilla, Rodi, Pfyshnet) nicht anonym, werden nicht mehr genutzt (Grapevine, Marabunta) oder sind nie wirklich zum Laufen gebracht worden (Crowds, Free Haven, Publius, Tangler, Turtle).

Entscheidende Eckdaten

Auch wenn die technischen Details und ihre Bedeutung für die Sicherheit Einfluss auf die Wahl eines anonymen P2P-Netzes haben, sind es doch häufig grundlegendere Faktoren, die die Entscheidung einschränken. Die Tabellen zeigen einige Eigenschaften der verschiedenen Netze.

Wie schon früher bemerkt wurde, können größere Netze theoretisch bessere Anonymität liefern; jedoch sind größere Netze auch häufiger Opfer gut ausgestatteter Angreifer. Ungewöhnlich schnelle Downloads können ein Zeichen sein, dass das Netz keine gute Anonymität erzeugt; natürlich sind schnelle Downloads und viele Suchergebnisse auch essenziell für die Benutzbarkeit.

Für Benutzer mit veralteten Rechnern können Speicher und CPU-Nutzung der Anwendung Relevanz haben. Die Daten in der Performance-Tabelle sind nur grobe Schätzungen – Entwickler anonymer Netze erschweren Messungen aus Sicherheitsgründen im Design der Protokolle. Einige der vorgestellten Netze machen es praktisch unmöglich, alle Knoten im Netz zu identifizieren. Die Anzahl an Suchergebnissen variiert je nach Wahl der Suchbegriffe und der Position des suchenden Knotens im Netz.

Eine weitere Möglichkeit zum Vergleich von P2P-Netzen bietet ihre Popularität, basierend auf Downloads. Freshmeat listed Softwarepopularität basierend auf Downloads, Abonnements für Benachrichtigungen für neue Versionen und der Anzahl der Treffer auf der Projektwebseite. Ältere Projekte haben natürlich mehr Treffer und werden daher als populärer gewertet. Die Tabelle Popularität listet die aktuellen Popularitätswerte zusammen mit den Daten der ersten und der neuesten Version für die verschiedenen hier vorgestellten P2P-Netze.

Die Features der verschiedenen vorgestellten P2P-Netze fasst die gleichnamige Tabelle zusammen. Gewisse Feinheiten gehen natürlich bei knappen Zusammenfassungen wie der hier vorgestellten verloren. Im Allgemeinen sind Netze mit Pfadwahl durch den Initiator sicherer – unter der Annahme, dass eine sichere Methode zum Finden von Knoten im Netz verfügbar ist. Künstliche Verzögerungen können die Anonymität verbessern, da sie die Verkehrsanalyse erschweren, jedoch leidet darunter die Geschwindigkeit.

Integritätsprüfungen auf Dateiebene können problematisch sein, falls das Netz es Feinden ermöglicht, ungültige Blöcke in den Datentransfer einzuspeisen, wie beim Swarming. Linkverschlüsselung bietet eine gewisse Grundsicherung gegen Verkehrsanalyse; Verschlüsselung auf Datenebene und möglicherweise Verschlüsselung von Suchanfragen schützen zusätzlich gegen neugierige Knoten im Netz. Integritätsprüfungen und Verschlüsselung sind relativ einfach zu implementieren und daher wahrscheinlich korrekt umgesetzt für die Netze, die in den Tabellen gelistet sind. Eine korrekte Umsetzung anonymer Pfadwahlmethoden ist deutlich komplizierter; Leser sollten nicht davon ausgehen, dass die verschiedenen Programme in dieser Hinsicht immer korrekt arbeiten.

Fazit

Tor und Mixminion sind in Bezug auf Sicherheit und Benutzbarkeit für anonymes Surfen beziehungsweise E-Mail die klaren Gewinner. Beim anonymen Dateiaustausch gibt es keinen eindeutigen Sieger – die Netze leiden durchweg an mangelnder Anwenderfreundlichkeit, zu kleiner Teilnehmerzahl oder Sicherheitsproblemen. Zudem können anonyme Netze mit der Geschwindigkeit und Benutzbarkeit nichtanonymer P2P-Netze nicht mithalten. So erhält man den Schutz der Privatsphäre nur unter Leistungsverlusten. (JS)

NILS DURNER

ist Anwendungsentwickler bei dmc digital media center. Er trägt zu verschiedenen GNU-Projekten wie GNUnet bei und ist Mentor beim Google Summer of Code. Weiterhin ist er Autor von PlibC, einer POSIX-Emulationsschicht für Windows.

NATHAN EVANS

ist Doktorand in Informatik an der Universität von Denver. Seine Forschungsinteressen gelten Computersicherheit, effizientem Routing und P2P-Systemen.

CHRISTIAN GROTHOFF

ist Professor für Informatik an der Universität von Denver. Seine Forschungsinteressen sind Compiler, Programmiersprachen, Netze und Computersicherheit. Er ist der Hauptautor von GNUnet, GNU's P2P Platform.

Literatur

[1] Nils Durner, Nathan Evans, and Christian Grothoff; yourshare: De-anonymizing the rshare network; crisp.cs.du.edu/youRShare/

[2] Nathan S. Evans, Chris Gauthier-Dickey, Christian Grothoff; Routing in the dark: Pitch black; in: ACSAC; IEEE Computer Society; 2007; S. 305 – 314

[3] Wei Dai; Pipenet; www.eskimo.com/weidai/pipenet.txt; 2003

[4] Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong; Freenet: A distributed anonymous information storage and retrieval system; in Hannes Federrath (ed.); De-signing privacy enhancing technologies: International Workshop on Design Issues in Anonymity and Unobservability; Berkeley/CIRCA; 25.–26.7.2000; proceedings volume 2009, 2001

[5] George Danezis, Roger Dingledine, David Hopwood, Nick Mathewson; Mixminion: Design of a type iii anonymous remailer protocol; in: IEEE Symposium on Security and Privacy, 2003

[6] Len Sassaman, Ulf Möller, Colin Tuckley, Eric Arneson, Alex Krik, Peter Palfrader; Mixmaster: an anonymous remailer; mixmaster.sourceforge.net, 2008

[7] Nils Durner, Nathan Evans, Christian Grothoff; Vielleicht anonym? Die Enttarnung von Stealthnet-Nutzern; c't 21/07, S. 218







Vertraulich drucken im Netz

Persönliche Zustellung

Dieter Michel

Die Nutzung zentraler Drucker kann bei der Ausgabe vertraulicher Dokumente heikel sein. Gefordert sind Verfahren, die nur autorisierten Benutzern Zugriff am Gerät ihrer Wahl gewähren.

Im Zuge eines Neubaus wurden bei der Roche Pharma AG die Bürobereiche als offene Flächen angelegt – inklusive frei zugänglicher Bereiche für die Druck- und Kopiersysteme, die als netzwerkfähige Geräte auf jeder Etage mehrfach vorhanden sind. Auf den ersten Blick nicht gerade technisches Neuland, doch möchte man gerne verhindern, dass die Anwender nach Absetzen eines Druckjobs zum Drucker spurten und dort ihre Aufträge womöglich noch zwischen denen der Kollegen suchen müssen. Das ist nicht nur unbequem und fehlerträchtig, sondern auch problematisch hinsichtlich eventuell vertraulicher Dokumente.

Ähnlich gelagerte Aufgabenstellungen gibt es in Sicherheits- und Finanzbehörden, Entwicklungsabteilungen und so fort. Die Lösungen tragen je nach Hersteller unterschiedliche Namen wie „Follow me printing“ oder „Print to me“. Letzteres ist die Bezeichnung von Ricoh, dem Anbieter eines entsprechenden Systems, das bei Roche zum Einsatz kam und Gegenstand dieses Berichts ist.

Das Prinzip: Der Anwender druckt zunächst in eine virtuelle Warteschlange, der Druckauftrag wird auf einem Druckserver zwischengespeichert und zum Ausdruck bereitgehalten. Benötigt der Anwender den Ausdruck, meldet er sich bei einem Drucker seiner Wahl mit dem RFID-Werksausweis an. Bei Roche stehen in jedem Stockwerk mehrere kombinierte Drucker-Scanner mit RFID-Lesegerät.

Auf dem LC-Display des Druckers erscheint nach der Benutzeranmeldung ein Menü, auf dem er einen oder mehrere seiner Aufträge zum Drucken auswählen (oder löschen) kann. Nach dem Ausdruck meldet er sich wieder ab.

Autorisierung durch RFID-Karte

Dahinter steckt eine Software des Bochumer Herstellers Genius Bytes, die speziell auf die Ricoh-Drucksysteme zugeschnitten ist. Basis ist die Embedded Software Architecture (ESA) von Ricoh, eine Java-Bibliothek, die es Drittanbietern ermöglicht, den Multifunktionsdrucker (MFP) an spezielle Anforderungsprofile anzupassen. Ricoh stellt dazu auch ein SDK zur Verfügung.

Ist der Benutzer via RFID autorisiert, kann er am Druckerpanel seine Aufträge verwalten.

Kernkomponenten sind der Imagus Document Server von Genius in Verbindung mit der Imagus Java-Anwendung, die auf jedem MFP installiert ist. Bei Roche kommen hier vor allem MFPs vom Typ Ricoh Aficio 3260C mit integriertem Scanner und Vorlageneinzug zum Einsatz.

Der Document Server verwaltet netzwerkweit die Druckaufträge. Bei Roche laufen zwei davon im produktiven Betrieb. Sie sind so ausgelegt, dass beim Ausfall eines Servers der andere die gesamte Last übernehmen kann. Dieser Server stellt auch den virtuellen Netzwerkdrucker bereit und verwaltet dessen Warteschlange. Die normale Windows-Queue ist zwar vorgeschaltet, leitet aber den Druckauftrag nur an den Server weiter, sodass eine Verwaltung von Druckaufträgen über die lokale Druckerverwaltung von Windows nicht möglich (und auch nicht erwünscht) ist.

Die Java-Anwendung kommuniziert auf der einen Seite mit dem RFID-Lesegerät des MFPs, auf der anderen mit dem Document Server. Dieser hat via Active Directory Kenntnis der netzweiten Accounts. Meldet sich ein Benutzer mit seinem Werksausweis am MFP an, übermittelt die Java-Anwendung auf dem Drucker zunächst die Ausweisnummer an den Document Server, der

wiederum aus dem Active Directory Benutzernamen und Zugriffsrechte ermittelt. Unter anderem kann er so feststellen, welche Aufträge des betreffenden Benutzers bereits warten und diese Informationen an die Java-Anwendung zurückmelden, die sie dem Anwender am Drucker präsentiert.

Firewall ist kein Hindernis

Über einen Zugriff auf den Document Server holt sich die Java-Anwendung die Daten und leitet sie an den lokalen Drucker weiter. Man beachte die Feinheiten: Nicht der Document Server selbst schickt auf Veranlassung der Java-Anwendung die Daten zun Drucker, sondern die Java-Anwendung holt sie sich. Das hat den Vorteil, dass das Konzept auch dann funktioniert, wenn die Drucker vom Server aus gesehen hinter einer Firewall stehen – zum Beispiel, um einen direkten Zugriff vom Netz aus auf die Drucker zu verhindern.

In ähnlicher Weise kann der Anwender über die Java-Anwendung die eigenen Druckjobs verwalten und etwa Einträge löschen. Zudem stellt der Imagus Document Server eine Weboberfläche zur Verwaltung bereit.

Wenn der MFP das unterstützt, kann die Java-Anwendung die Scanner-Einheit für Dienste wie Scan-to-Mail oder Scan-to-Fax nutzen. Dafür ist der Document Server selbst nicht erforderlich, sondern nur der Active-Directory-Zugriff, um die E-Mail-Adresse des Benutzers und seine Zugriffsrechte auf Netzwerk-Shares oder Faxserver zu ermitteln. Das Imagus-Programm kommuniziert dazu mit der jeweiligen Anwendung oder legt die gescannten Daten auf einem für den Benutzer lesbaren Netzlaufwerk ab und verschickt eine Benachrichtigung per E-Mail. Auch das lässt sich über das Imagus SDK einrichten.

Der in einer virtuellen Maschine laufende Ricoh Websmart Device Monitor fragt in regelmäßigen Abständen die MFPs ab, überwacht den Tonerstatus und dergleichen und verschickt auf Wunsch Warnungen an die Support-Verantwortlichen. Bei Roche nutzt man das, um den Vermieter der MFPs über Servicebedarf zu informieren. (JS)

DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.





Marktübersicht: Unified Communications

Überall und jederzeit



Barbara Lange

Unified Communications ist modern, vielleicht sogar ein Hype. Auf jeden Fall werben viele Unternehmen aus unterschiedlichen Bereichen mit der Vereinheitlichung verschiedener Kommunikationskanäle unter einer Oberfläche. Eine Marktübersicht.

Der Unified-Communications-Markt ist unübersichtlich. Viele Marktteilnehmer wollen die Kommunikation aus ihrer Perspektive vereinheitlichen: Zum einen drängen Softwarehersteller in den Telefoniemarkt. So bietet Microsoft mit seinem Office Communications Server 2007 ein Unified-Communications-Paket inklusive Instant Messaging, Präsenzmanagement, Audio-, Web- und Videokonferenzen an.

Gleichzeitig erweitern Telekommunikationsanbieter ihre PBX-Anlagen um UC-Funktionen. Darüber hinaus versuchen Hardwarehersteller, IP-Telefonie-Anbieter, Systemintegratoren und Berater, ihren Teil vom Kuchen zu ergattern.

Das alles macht eine Definition von Unified Communications nicht leicht. Daran arbeitet derzeit der Verband der deutschen Internetwirtschaft e. V. eco in seinem Arbeitskreis für UC, den er Ende 2007 gegründet hat.

Demnach ist unter „Unified Communications“ die Integration und Automatisierung der gesamten Unternehmenskommunikation zu verstehen, und zwar bezogen auf vier Aspekte.
Medien: (Video-)Telefonie, E-Mail, Instant Messaging, Fax, Brief, SMS/MMS, Websites, Telefon-, Video- und Webkonferenzen, Chat;
Netze: IP-Netze (Licht, Draht, Funk), PSTN;
Routing- und Automatisierungsbausteine: IVR- und Sprachdialogsysteme, E-Mail-Management, Automatic Call Distribution, Dialer;
Applikationen: ERP, CRM, Content Management, Dokumentenmanagement [a].

Damit geht Unified Communications weit über das seit Jahren bekannte Unified Messaging hinaus, das sich in der Regel mit der Integration von Sprache, Fax, SMS und E-Mail begnügte. Hinzugekommen sind die Echtzeitkommunikation, das Präsenzmanagement, die Integration in Systeme wie Microsoft Outlook, Lotus Notes und CRM-Funktionen. Die Krönung ist eine fortgeschrittene Zusammenarbeit von Teams durch Konferenzfunktionen, Diskussionsforen, Application Sharing oder Teamkalender. Dann kann man per Mausklick Konferenzen einberufen, ist immer unter ein und derselben Nummer erreichbar und auch im mobilen Einsatz nahtlos angebundener Bestandteil der Unternehmenskommunikation.

In der Theorie zumindest. Nach Einschätzung der Tagung „Praxis und Wunschdenken zu Unified Communications“ des eco-Arbeitskreises Anfang Mai [e] sind zwar alle Einzelkomponenten technisch ausgereift. Die komplette Integration aber lässt noch Fragen offen. Derzeit gibt es nach Meinung von Branchenkennern wenige Installationen, die nicht nur auf dem Papier alle Möglichkeiten integrieren. Realisiert sind oft nur Teilaspekte, zudem sollte man die organisatorischen Herausforderungen nicht unterschätzen.

Auch die Marktübersicht (S. 100) verdeutlicht, dass die einzelnen Anbieter die UC-Funktionen in unterschiedlichem Maße umsetzen. Während sich einige auf Unified-Messaging-Funktionen konzentrieren, liefern andere ein vollständig integriertes System, vor allem die Großen wie Microsoft, IBM, Nortel oder Siemens.

Von Inseln und Global Players

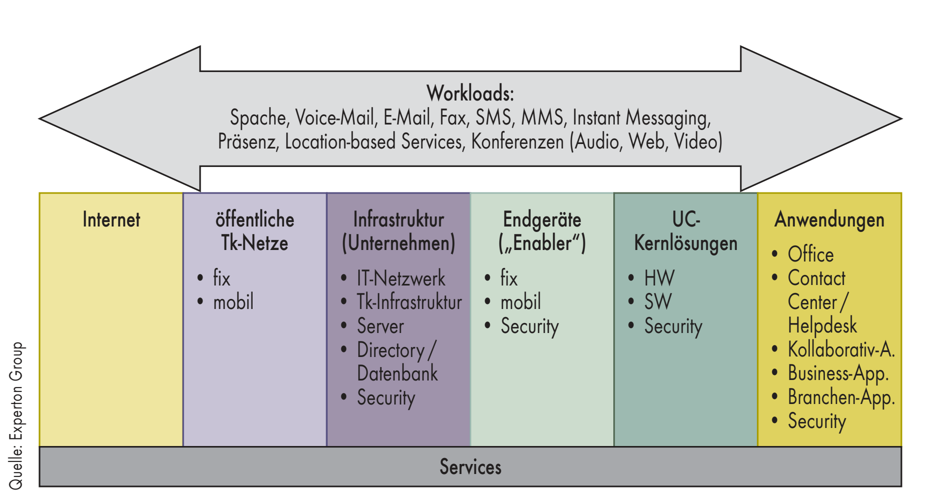
Nach Einschätzung der Experton Group (www.experton-group.de) ist der Markt in Deutschland dadurch geprägt, dass sich für jeden Kanal Insellösungen herausgebildet haben und vor allem Cisco und Microsoft neue Techniken vorantreiben.

Entgegen den Aussagen des Marketings prophezeien die Analysten „nur“ eine evolutionäre Entwicklung und eine bis 2010 andauernde Pilotphase, in der

die Standards weiter heranreifen würden. Mit einem Durchbruch rechnen die Analysten folgerichtig erst zum Ende der Dekade. Und: Der Markt bleibe bis auf Weiteres fragmentiert.

Dass der UC-Markt nicht nur anbieter-, sondern auch anwendergetrieben ist, stellt Berlecon Research in seiner Studie „Wettbewerbsfaktor effiziente Kommunikation – Potenzial von Unified Communications“ [b] fest. Nach der von Damovo und Nortel beauftragten Untersuchung halten 56 Prozent der Anwender UC für sinnvoll, sind gleichzeitig aber nur von der Vereinheitlichung und Integration ihrer Kommunikation zu überzeugen, wenn Softwarehersteller, TK-Systemhäuser und Festnetzprovider ihre Kompetenzen bündeln.

In Teilbereichen gibt es die geforderte Anbieterkooperation durchaus. So arbeiten Nortel und Microsoft beispielsweise in der Innovative Communications Alliance (www.innovativecommunicationsalliance.com) zusammen mit dem Ziel, Microsofts OCS und den Exchange Server mit Nortel-Systemen zu integrieren. Dafür wird die Telefonanlage mit OCS ohne Gateway gekoppelt. Mit der Integration von Nortel- und IBM-Produkten ist man derzeit im Joint Development Center in North Carolina beschäftigt.



Unified Communication vereinigt die gesamte Kommunikationsstruktur (Abb. 1).

Globale Arbeitsweise virtueller Teams

Entwickelt wird dort auch ein Integrations-Framework namens Agile Communication Environment (ACE), das in zwei bis drei Monaten herauskommen soll. „Damit sind wir allein auf weiter Flur“, so Martin Ruoff von Nortel. ACE soll IBM- und Microsoft-Lösungen einbinden. Geplant ist darüber hinaus eine Branch-Office-Version, das heißt, ein Router speziell für Zweigstellen, die im zentralen Rechenzentrum versorgt werden. Der Router beinhaltet auch OCS und springt an, wenn das zentrale Netz einmal ausfällt.

Doch oft genug müssen die Anbieter viel tiefer ansetzen und dem potenziellen Kunden erst einmal verdeutlichen, was für den Einsatz von Unified Communications spricht. Gern genannt werden:

Zukunftschancen: Virtuelle überregionale Teams und flexible Arbeitsmodelle sowie eine zunehmende Mobilität durchbrechen starre Organisationsformen und Kommunikationsstrukturen.

Kommunikationseffektivität: Medien wie E-Mail schüren die Erwartung einer schnellen Reaktion – auf Kundenanfragen zum Beispiel. Auch die Kommunikationsmenge steigt, wird aber von einer gleichbleibenden oder sinkenden Anzahl von Mitarbeitern bewältigt, wie die besagte Berlecon-Studie feststellt. Mit einer Vereinheitlichung der Kommunikationskanäle könnte man diesen höheren Anforderungen begegnen.

Echtzeitkommunikation via Instant Messaging oder Videokonferenzen sind hierzulande noch nicht breit im Einsatz. Das soll sich aber bald ändern, glaubt man der Studie „The Hyperconnected: Here They Come!“, die IDC im Auftrag von Nortel erstellt hat [c]. Demnach sind es nicht nur die Unternehmen, die etwas von ihren Angestellten erwarten, sondern vor allem die Extrem- und Intensivnutzer, die etwas von ihrem Arbeitgeber erwarten.

Sogenannte Extremnutzer haben mindestens sieben verschiedene Endgeräte und mindestens neun Kommunikationsapplikationen (IM, SMS, Webkonferenzen etc.) im ständigen Gebrauch. 16 Prozent der Beschäftigten gehören dazu (befragt wurden 2400 Menschen aus 17 Ländern).

36 Prozent sind Intensivnutzer mit mindestens vier Endgeräten und sechs Kommunikationskanälen. Die Marktforscher schließen daraus, dass Unternehmen perspektivisch zum Einsatz von Unified Communications nahezu gezwungen sein werden – und zwar vor allem in Asien. Aber auch hierzulande nutzt die nachwachsende Generation Echtzeitkommunikation wie Instant Messaging so selbstverständlich, dass sie das sicherlich in Zukunft im Arbeitsprozess nicht missen will.

Nicht-Erreichbarkeit kostet Geld

Dass schlechte Erreichbarkeit und eine fragmentierte Kommunikationsstruktur im Unternehmen richtig Geld kosten können, hat Siemens Enterprise Communications in der in Nordamerika und Europa durchgeführten Studie „Measuring the Pain: What is Fragmented Communication Costing Your Enterprise?“ [d] im Jahr 2007 quantifiziert und ausgerechnet, dass Unternehmen mit 1000 Beschäftigen unter Umständen mehr als 13 Millionen US-Dollar pro Jahr für „schlechte“ Kommunikation ausgeben. Was Geld kostet: Warten auf Informationen von anderen (5,3 Stunden pro Woche), fehlende Arbeitswerkzeuge an externen Standorten (7,8 Stunden pro Monat), unnötige Geschäftsreisen.

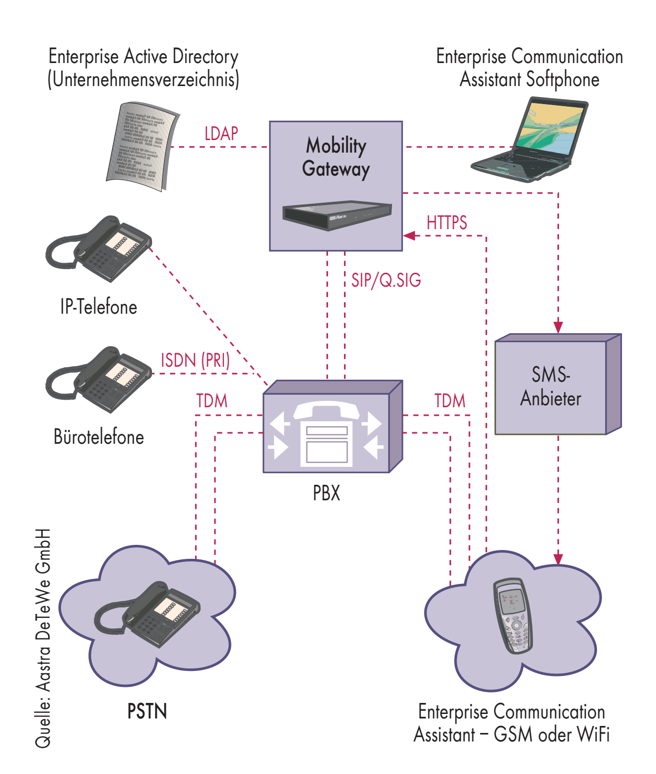
iX-TRACT

- Unified Communications soll die gestiegenen Anforderungen an die Kommunikation durch eine Vereinheitlichung der Kanäle lösen. Noch ist der Markt fragmentiert, es gibt erste Kooperationen.
- Technische Anforderungen liegen in der Integration von Medien und Netzen unter einer Oberfläche, in der Einbindung mobiler Mitarbeiter und der Kommunikation über Unternehmensgrenzen hinweg.
- UC-Applikationen verändern die internen Kommunikationsprozesse in Unternehmen – technisch, organisatorisch und sozial.

Anbieter von Unified-Communications-Lösungen

Hersteller	Produkt	Funktion
Aastra DeteWE	Enterprise Mobility Gateway (Hardware)	Integration mobiler Geräte
	Unified Communication Platform UCP (Software)	Voice, E-Mail, Fax, mobile Geräte, Präsenzmanagement, IVR, Remote-Zugriff auf alle Nachrichten via Webbrowser, PDA
Alcatel-Lucent	Omnitouch Unified Communications (My Teamwork, My Messaging, My Phone and My Assistant)	Voice, E-Mail, Fax, mobile Geräte, Konferenzen (Telefon)
Avaya-Tenovis	Avaya one-X-Mobile, one-X–Portal, one-X -Mobile Edition, Modular Messaging, Mobility Manager, Meeting Exchange Express, C3000 Messaging	Voice, E-Mail, Fax, Instant Messaging, mobile Geräte, Konferenzen (Telefon, Video), CTI, VoIP, MS Outlook, Lotus Notes
	Intelligent Presence	Präsenzmanagement; Integration mit MS OCS
Avodaq AG	Integration von Cisco-Lösungen	basierend auf Cisco-Lösungen
CAE Elektronik GmbH Stolberg	Caesar (Software)	Integration von Voice-Mail, E-Mail, Fax, SMS, MMS, Instant Messaging, Präsenzmanagement, CTI, VoIP, SAP, Goupwise, IBM Sametime, MS OCS
C4B Com for Business AG	Xphone-Produktpalette	Voice, E-Mail, Fax, SMS, mobile Geräte, Präsenzmanagement, CTI, MS Outlook, Lotus Notes
Cisco	umfassende Produktpalette für Unified-Communications-Lösungen, z. B. Cisco Unified Communication Manager, Unified Personal Communicator, Unified Mobility Manager, Unified Videoconferencing, Unified Meetingplace Express, Unified Presence Server	Voice, E-Mail, Fax, SMS, IM, mobile Geräte, Konferenzen (Audio, Video, Web), Präsenzmanagement, CTI, VoIP, IVR, MS Outlook, Lotus Notes
Cytel Technology AG	CYTEL.iBX	softwarebasierte VoIP-Telefonanlage; Integration Voice-Mail, Fax, SMS, IM, mobile Geräte, Präsenzmanagement, CTI, IVR, VoIP, MS Outlook
Cycos AG	Cycos mrs (Software)	für Contact-Center: Voice-Mail, E-Mail, Fax, SMS, mobile Geräte, Konferenzen (Telefon, Video), CTI, VoIP, IVR, MS Outlook, Lotus Notes, SAP
Datac Kommunikationssysteme	Unified Communication	Voice, E-Mail, Fax, SMS, mobile Geräte, CTI, VoIP, Outlook, SAP, Groupwise, Navision, IBM AS/400 Lotus, MS Exchange
Damovo	Systemintegration	Systemintegration
Digitronic Computersysteme	Shark	Voice, E-Mail, Fax, SMS
Estos GmbH	Estos Procall 3.0 Enterprise	Voice, E-Mail, IM, mobile Geräte, Konferenzen, Präsenzmanagement, VoIP, CTI, MS-Outlook, Exchange, Lotus Notes
Experton Group AG	Marktforschung und Beratung	
Ferrari electronic AG	Office Master 3.1 (Software)	Voice, E-Mail, Fax, SMS, mobile Geräte, CTI, VoIP, IVR, MS Outlook, Lotus Notes, SAP Workplace, Exchange 2007
	Office Master Gate (Hardware)	verbindet Microsoft Exchange Server 2007 und OCS 2007 mit ISDN-TK-Anlagen
IBM	Soft- und Hardware im Rahmen der Unified-Communications- und Collaboration-Strategie (UC2); System-i-Unified-Communications	komplettes UC-Spektrum
infoWAN Datenkommunikation GmbH	Integration	Implementierung auf der Basis von Microsoft-Produkten, z. B. OCS
MCA GmbH Gesellschaft für Kommunikationslösungen	Konvi CTI (Software)	Voice, E-Mail, Fax, SMS, IM, Präsenzmanagement, CTI, VoIP, IVR, MS Outlook, Lotus Notes, Groupwise, IBM Lotus Sametime, SAP R3
Microsoft	Office Communications Server 2007, Office Communicator 2007 (Client)	Voice, E-Mail, SMS, IM, mobile Geräte, Konferenzen (Telefon, Video), Präsenzmanagement, CTI, VoIP, Outlook
MKS Kommunikationssysteme	Advanced Unified Messaging-Server	Voice, E-Mail, Fax, SMS, IM, CTI, MS Exchange, Lotus Notes, Novell Groupwise
Niggemann Innovations	Office Edition	Voice, E-Mail, Fax, SMS, Office EDITION integriert Fax, Voice, Mail, SMS, CTI, VoIP; MS Outlook, Lotus Notes, SAP
Nortel	Mobilex	für KMU – Einbindung mobiler Mitarbeiter
	Soft Communication Server 500	Soft- und Hardware-Lösung, IM, Präsenzmanagement Voice-Mail
serVonic	IXI UMS	Voice, E-Mail, Fax, SMS, IM, Präsenzinformationen, CTI, VoIP, MS Outlook, Lotus Notes
Siemens Enterprise Communications	Openscape Unified Communications	Voice, E-Mail, Fax, SMS, IM, Konferenzen (Telefon, Video); Präsenzmanagement, CTI, VoIP, MS Outlook, Lotus Notes, ERP
Swyx Solution AG	SwyxVoicemail, SwyxFax, SwyxCTI, SwyxECT, SwyxMobile, SwyxIT!, SwyxConference	Voice, E-Mail, Fax, mobile Geräte, Konferenzen (Telefon), CTI, VoIP, MS Outlook, Lotus Notes
thetakom. telekommunikationssysteme gmbh	Integration: mrs von Cycos und Cisco Unified Communications	Cycos und Cisco
Vipcom AG	Papageno (Softwarelösung)	Voicemail, E-Mail, Fax, SMS, VoIP, MS Outlook, Lotus Notes
Voxtron GmbH	agenTel 6.1 (Softwarelösung)	softwarebasierte Contact-Center-Lösung; E-Mails und Telefonate unter einer Oberfläche, skill-basierte Weiterleitung, Integration in vorhandene Telefonanlagen

Kerngeschäft	Link
Hersteller von ITK-Kommunikationslösungen	www.aastra-detewe.de
Telekommunikationsausrüster	www.alcatel.de
Telekommunikationsausrüster	www.avaya.com
Systemintegrator	www.avodaq.de
Anbieter von Simulations-systemen und Unified-Communications-Systemen	www.cae-stolberg.de
Hersteller von Telefonie- und Kommunikationslösungen	www.c4b.de
Netzausrüster	www.cisco.de
VoIP-Hersteller	www.cytel.de
Softwarehersteller	www.cycos.de
System- und Softwarehaus	www.datac-gmbh.de
Systemintegrator	www.damovo.de
IT-Hersteller	www.digitronic.net
Entwicklung von Produkten im Bereich Telekommunikation	www.estos.de
Martkforschung und Beratung, Schulungen	www.experton-group.de
Hersteller von Unified-Messaging-Systemen	www.ferrari-electronic.de
IT-Hersteller	www.ibm.de
Beratung und Implementierung von IT-Systemen	www.infowan.de
IT-Hersteller	www.mca-gmbh.de
Softwarehersteller	www.microsoft.de
Systemintegrator	www.mks.at
IT-Hersteller	www.niggemann-innovations.de
Telekommunikationsausrüster	www.nortel.de
Softwarehersteller	www.servonic.de
IT-Hersteller	www.enterprise-communications.siemens.com/deutschland/default.aspx
IP-Telefonieanbieter	www.swyx.de
Systemhaus; Integration von Kommunikations- und Messaging-Lösungen	www.thetakom.de
Softwareentwicklung, Systemintegrator	www.vipcomag.de
Entwicklung von Software für Callcenter und Sprachportale	www.voxtron.de



Das Mobility-Gateway von Aastra DeTeWe: Mobile Geräte als Nebenstelle (Abb. 2).

Als technische Basis von UC haben sich IP-Netze herauskristallisiert. Die Analysten von Berlecon sehen in einer anderen Studie („VoIP und Unified Communications 2008“) VoIP als Voraussetzung für Unified Communications, da unter technischen und wirtschaftlichen Gesichtspunkten nur dann eine Integration sinnvoll sei. Mehr als die Hälfte der Unternehmen nutzt aber gar kein VoIP.

Als eine Herausforderung gilt noch die Einbindung mobiler Endgeräte in UC-Projekte. Im Mai dieses Jahres hat Aastra Detewe die Kommunikationssparte von Ericsson übernommen und bietet nun das „Enterprise Mobility Gateway“ (Abb. 2), eine Hardware, die die Verbindung zwischen mobilen Endgeräten und dem Unternehmensnetz herstellt. Ziel ist es, dass Mitarbeiter vom mobilen Gerät aus Funktionen nutzen können, die bislang nur am PC oder an der TK-Anlage möglich waren. Derzeit unterstützt das der mobile Client Symbian, mit der nächsten Release auch Windows Mobile und Blackberry.

Nortel hat „MobileX“ für die Einbindung von mobilen Mitarbeitern entwickelt. Damit ist das Handy in Microsoft-Umgebungen in die Unternehmensumgebung integrierbar, sofern der Provider „Server based Routing“ unterstützt. Die Anrufe landen dann zunächst bei der Unternehmens-PBX, sowohl Festnetztelefon als auch Handy klingeln. Geht der Mitarbeiter ans Handy, zeigt das Festnetzgerät „besetzt“.

UC ist nicht nur Technik

Die Bereiche Mobilität und die Kommunikation über Unternehmensgrenzen hinweg sieht auch Kai Riemer vom European Research Center for Information Systems (ERCIS) (www.ercis.de) als Herausforderungen im technischen Bereich. Noch gebe es für die Einbindung mobiler Mitarbeiter keine Standards. Das Dilemma: Zwar bieten die UC-Systeme umfassende Infrastrukturen, die sind aber mobil und über das Unternehmen hinausgehend nur eingeschränkt nutzbar.

Was oft vergessen wird: Unified Communication ist mehr als eine Vereinheitlichung von bislang getrennten Kommunikationskanälen, wie das Beispiel Präsenzmanagement zeigt. Die Frage, ob sich Mitarbeiter unterstützt oder überwacht fühlen, wenn alle Kommunikationsteilnehmer wissen, ob und wie man gerade erreichbar ist, scheint noch nicht entschieden. Hier spielen neben technischen Fragen auch rechtliche und psychologische Faktoren eine Rolle. (JS)

BARBARA LANGE

ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz&einfach in Lengede.

Onlinequellen

[a] www.eco.de/arbeitskreise/unified-communications.htm

[b] www.berlecon.de/potenzial_uc

[c] White Paper IDC: „The Hyperconnected – Here They Come!“ sponsored by Nortel; May 2008 – Download (nach Anmeldung); www.nortel.com/promotions/idc_paper/index.html

[d] „Measuring the Pain: What is Fragmented Communication Costing Your Enterprise?“; Download nach Anmeldung; www.siemens.de/open/ucsurvey

[e] eco-Tagung „Praxis und Wunschdenken zu Unified Communications“; www.eco.de/veranstaltungen/202_4906.htm





25 Jahre BTX

Vorlauf

Detlef Borchers



Am Anfang des Online-Lebens und E-Commerce in Deutschland stand die deutsche Post – mit dem von ihr angebotenen Bildschirmtext, der jetzt 25 wäre.

Am 2. September 1983, am Vorabend der Berliner Funkausstellung, startete die deutsche Bundespost den Bildschirmtext, der Deutschland (West) zu einem Volk der „Teleleser“ machen sollte. Bis 1985, so die Vorgabe des insgesamt auf 200 Millionen D-Mark veranschlagten Gesamtprojekts, sollte sich jeder Bundesbürger zum Ortstarif in ein bundesweites Netz einwählen können und politische Informationen, Fahrpläne sowie Sportnachrichten abrufen und dem Telekauf per Schaltstern („*#“) frönen können. Teleshopping bei Neckermann, Otto und Quelle, Onlinebanking bei der Norisbank – der Telekauf sollte den Bundesbürgern die Vorteile eines neuen Online-Lebens schmackhaft machen. 21 329 Haushalte, dazu 3000 Feldversuchsteilnehmer ließen sich im ersten Jahr darauf ein, über das Telefonnetz mit einem „BTX-Modem“ am Fernseher ein Onlinesystem zu benutzten, das mit farbiger Klötzchengrafik arbeitete.

Zum offiziellen Start auf der internationalen Funkausstellung (IFA) konnte BTX bereits auf eine bewegte Geschichte zurückblicken. Denn schon auf der IFA 1977 freute sich der damalige Postminister Kurt Gscheidle, das britische Viewdata-System präsentieren zu können, aus dem nach einer Idee im Postministerium BTX werden sollte. Dass es sechs Jahre statt wie geplant ein Jahr dauerte, bis BTX starten konnte, lag erstens am erbitterten Widerstand der Zeitungsverleger, die in den von Gscheidle gepriesenen „Online-Nachrichten“ eine Bedrohung ihrer wirtschaftlichen Grundlagen sahen. Außerdem lag es an einer Ausschreibung der Datenverbundtechnik, die überraschend IBM gewinnen konnte, obwohl man keinerlei Erfahrungen mit einem solchen System hatte. Prompt konnte IBM sein System nicht zum vorgesehen Starttermin im September 1983 liefern, weswegen die Post bis Juni 1984 auf das alte Viewdata-System zurückgreifen musste.

Terminal mit Fernsehen gekreuzt

Die Idee zu Viewdata kam dem englischen Ingenieur Sam Fedida vom Post Office Research Centre, als er ein Memorandum der amerikanischen Wissenschaftler Licklider und Taylor gelesen hatte. Ihr Text „The Computer as Communications Device“ aus dem Jahre 1968 gilt heute als theoretische Geburtsstunde des Internet. Genauso wichtig war er für die Entwicklung des BTX-Systems. Fedida beschäftigte sich damit, wie man ein Computerterminal mit einem Fernsehgerät kreuzen könnte. Sein „Viewdata Timesharing Common Carrier“ genanntes System wurde im September 1975 der Öffentlichkeit vorgestellt und bald in Prestel ungetauft, benannt nach der Klötzchengrafik, die das System produzierte. Dieses Prestel-System wurde 1977 in Deutschland vorgeführt und stieß auf riesiges Interesse. „Eins zu Null für die Bundespost“ titelte ein großes deutsches Wochenmagazin. 120 Firmen meldeten auf der IFA ihr Interesse an Bildschirmtext.

Auf der IFA 1979 konnte die Bundespost 123 Firmen präsentieren, zum Start des BTX-Feldversuches im Jahr 1980 gar 300 Anbieter, zum Publikumsstart 1983 waren es 344. Alle hofften auf das große Onlinegeschäft zu niedrigen Kosten. Abgesehen vom Telefon-Ortstarif, damals 20 Pfennig für 24 Stunden, sollten nur wenige Seitenabrufe kostenpflichtig sein, weil der erwartete Telekauf alles subventionieren sollte. Firmen sollten „Schlagworte“ kaufen, so die ursprüngliche Idee. Gab der BTX-Teilnehmer das Schlagwort mit dem „Schaltstern“ ein (zum Beispiel *Heise#), landete er auf dem Angebot der Firma.

Allerdings stellte sich schon 1984 Ernüchterung ein: Die Produktion von BTX-Decodern für die Fernsehgeräte und Modems verlief schleppend, ihre Preise waren viel zu hoch. Statt der 300 000 prognostizierten Teilnehmer verfügten nach einem Jahr nur 38 894 Haushalte über BTX (die 300 000er-Grenze wurde 1991 übersprungen). Wirklich erfolgreich war nur das Onlinebanking, das vor allem Kleinbetriebe nutzten – und Beate Uhse. Die Firma kaufte von Beginn an so viele nicht-erotische Schlagworte wie nur irgend möglich. Sie sollten alle zu dem einen Onlinekatalog führen. Weil die BTX-Seiten dem Suchenden alphabetisch geordnet präsentiert wurden, besaßen die Flensburger Sexshopbetreiber in ihren besten BTX-Zeiten Hunderte von Firmen wie „AAAAAAA Aktuelle Information“. Der Rekord war eine Handelsregister-Eintragung mit 500 As vor dem Namen. Kürzer ausgedrückt: Sex sells.

Leuchtturm für die Nachbarn

EDV-technisch sollte das deutsche BTX eine „Leuchtturmfunktion“ für andere Länder haben, wie man heute sagen würde. SEL, der Hoflieferant der Post, schickte ein SELTEX genanntes System in die Ausschreibung, das ein eng vermaschtes Netz von 400 verteilten, im Stil des Arpanet gekoppelten Servern vorsah. Demgegenüber propagierte IBM einen hierarchischen Netzaufbau nach dem SNA-Prinzip mit einem Zentralrechner in Ulm, der alle regionalen Datenbanken enthielt und reihum 50 Regionalzentren bediente. Das IBM-System war mit 30 Millionen Mark wesentlich billiger als SELTEX, wobei IBM vor allem dadurch gewann, dass es den Inhaltsanbietern Pfennigbeträge für BTX-Seitengebühren versprach. IBM wollte Mehreinnahmen vor allem durch die Lizenzierung des IBM-Protokolls EHKP (Einheitliches Höheres Kommunikationsprotokoll) erzielen, mit dem Fremdrechner an BTX angeschlossen wurden. Für IBM war der Start ein mittleres Fiasko: Die Firma

hielt als Generalunternehmer für den gesamten Rechnerverbund den Termin vom 2. September nicht ein und zahlte eine Konventionalstrafe von 3,6 Millionen Mark. Erst 1993 konnte IBM mit der (nunmehr veralteten Technik) einen Gewinn erzielen.

Dauerbrenner Onlinebanking

Die Entwicklungsgeschichte von BTX ist eng mit dem Onlinebanking verbunden, das bis zum offiziellen Ende des Bildschirmtextdienstes im Jahr 1999 die dominierende Anwendung war. Tatsächlich lief BTX wegen zahlreicher wechselunwilliger Bankingkunden als „T-Online Classic“ munter weiter und wurde erst am 10. Mai 2007 während einer feierlichen „Power Off“-Veranstaltung in Ulm abgeschaltet. In dieser Hinsicht erlebte der älteste deutsche Onlinedienst auch das, was die BTX-Techniker als „BTX-Depression“ bezeichneten: Im November 1984 erleichterte der Chaos Computer Club mit einem Trick die Hamburger Sparkasse (Haspa) um 135 000 DM: Die Hacker ließen die Haspa für jeweils 9,97 Mark 14 Stunden lang den Text „Es erfordert ein bemerkenswertes Team, den Gilb zurückzudrängen“ abrufen. Mit Gilb war die deutsche Bundespost gemeint, der Betreiber des BTX-Systems, den Hacker wegen seiner restriktive Modem-Zulassungspraxis hassten.

In der fast 30-jährigen Existenz von BTX gelang es dem durchaus aufgeschlossenen Gilb nicht, aus dem deutschen Volk ein Volk der Teleleser zu machen, wie 1983 versprochen. Das lag auch an der technischen Entwicklung. Die Techniker der Post begriffen zu spät, dass der Personal Computer dem BTX-Fernseher weit voraus war; und sie waren zu stark von der Technik abhängig, die IBM lieferte. Als man 1992 soweit war, die Klötzchengrafik durch einen grafisch ansprechenderen „Kit-Standard“ zu ersetzen, hatten Onlinedienste wie Compuserve und AOL schon viele „Onliner“ in Deutschland gebunden. Und mit dem kommerziellen Internet wurde die ganze Welt zum Teleleser. (hb)

DETLEF BORCHERS

ist freier DV-Journalist und arbeitet für deutsche und amerikanische Fachzeitschriften.



Mailadressen genießen einen besonderen Schutz

Namentlich

Tobias Haar

E-Mail-Adressen bestehen häufig aus Namensbestandteilen oder aus anderen griffigen oder gar bekannten Kennzeichen oder Marken. Wer hier die Rechte Dritter übersieht, kann sich schnell juristischen Ärger einfangen.

Rechtliche Auseinandersetzungen um Domainnamen gehören mittlerweile zur Routine im Bereich des IT-Rechts. Deutlich seltener kommt es zu juristischen Auseinandersetzungen um E-Mail-Adressen. Aber es gibt sie, wie das unter IT-Juristen bekannte „Maxem“-Urteil zeigt (dazu später mehr). Um sich der juristischen Bewertung der Rechte an den Bestandteilen einer E-Mail-Adresse zu nähern, muss man zunächst klären, ob den Bestandteilen einer E-Mail-Adresse vor dem „@“ – dem „Local Part“ – ein anderer rechtlicher Schutz zusteht als den Bestandteilen nach dem „@“, der Domain. Grundsätzlich ist das nicht so. Es kommt für die rechtliche Bewertung nicht darauf an, ob eine Bezeichnung, ein Name, eine Marke oder eine sonst wie „namensrechtlich“ geschützte Zeichenfolge vor oder nach dem At-Zeichen stehen.

Die zentrale Vorschrift des Namensrechts, die für alle Bestandteile einer E-Mail-Adresse einschlägig sein kann, enthält der § 12 des Bürgerlichen Gesetzbuches (BGB). Sie regelt fast schon lapidar, dass bei einer Verletzung des Namensrechts der Berechtigte vom Verletzer Beseitigung beziehungsweise Unterlassung dieser Verletzung verlangen kann. Hinzu kommen Schadensersatzforderungen, und in krassen Fällen kann auch das Strafrecht greifen. Was das Namensrecht aber im Einzelnen umfasst, regelt die Vorschrift nicht. „Der Name ist die sprachliche Kennzeichnung einer Person, durch die sie von anderen unterschieden wird. Er ist Ausdruck der Individualität und dient der Identifikation des Namensträgers.“ So steht es im Münchener Kommentar zu § 12 BGB. Wichtig ist dabei, dass auch die Vermögensinteressen des Berechtigten an der Verwertung des Namensrechtes geschützt sind. Dies hat der Bundesgerichtshof anhand des Namens „Marlene Dietrich“ entschieden.

Namensrechtliche Vorschriften enthalten auch das Handelsgesetzbuch, das Gesetz gegen den unlauteren Wettbewerb und das Markengesetz. Dadurch sind etwa auch Firmennamen „namensrechtlich“ geschützt. Die Regeln ähneln einander stark, sodass es in den meisten Fällen nicht darauf ankommt, ob eine natürliche (Privat-) Person oder eine Firma gegen Namensverletzungen vorgeht.

Local Part ungleich Domain

So eindeutig die gleiche juristische Betrachtung der E-Mail-Adressbestandteile vor und nach dem „@“ erscheint, so verwirrend ist dann die Information, dass dies doch nicht immer der Fall sein muss. Das zeigt der „Maxem-Fall“. Ein Rechtsanwalt namens Maxem klagte gegen den Nutzer der Domain maxem.de sowie – und das macht den Fall besonders – mehrerer E-Mail-Adressen, die den Bestandteil „maxem“ enthielten. Der Beklagte wurde ausdrücklich darauf verklagt, die Bezeichnung „maxem“ auch nicht in Form einer E-Mail-Adresse zu nutzen – und zwar gleich, ob „maxem“ vor oder nach dem At-Zeichen eingesetzt wurde.

Hinsichtlich der Domain maxem.de entschied der Bundesgerichtshof, dass dem Träger des Namens „Maxem“ ein Unterlassungsanspruch gegen einen Nutzer dieser Bezeichnung zusteht, der kein Namensrecht geltend machen konnte. Dagegen aber „wird das Interesse des Klägers nicht durch jede Verwendung des Namens oder Namensbestandteils „maxem“ im Rahmen einer E-Mail-Adresse tangiert“, so die Richter. Wie so oft in der Juristerei kommt es auch hier nach Meinung der höchsten deutschen Zivilrichter – zu Recht – auf den Einzelfall an. Dem Namensträger wird durch die Registrierung der Domain maxem.de durch einen Nicht-Namensträger die Möglichkeit genommen, unter dieser Domain einen eigenen Internet-Auftritt zu gestalten.

In der Sprache der Richter heißt es, dass „ihm durch die Registrierung seines Namens als Internet-Adresse zugunsten des Beklagten dieser Namensgebrauch streitig gemacht“ wird. Selbstverständlich führt dieses Verbot der Domainnutzung dann auch zum Verbot der Nutzung von E-Mail-Adressen unter dieser Domain (zum Beispiel maxem@maxem.de oder info@ma xem.de). Die rechtliche Situation einer Domain hat also in der Regel immer auch entsprechende Auswirkungen auf die unter dieser Domain existierenden E-Mail-Adressen. Dass dies auch technisch in der Regel erforderlich ist, um E-Mails eindeutig einem Mailserver

zuweisen zu können, spielt dabei namensrechtlich keine Rolle.

Spannenderweise haben die Richter aber ausdrücklich nicht die Nutzung des Namens „maxem“ in anderer Form in E-Mail-Adressen untersagt. So durfte der Beklagte auch weiterhin E-Mail-Adressen à la „maxem@example.com“ benutzen. Dies jedenfalls, solange davon keine Interessen des Namensinhabers berührt sind.

Wer zuerst kommt, freemailt zuerst

Steht kein Namensrecht eines Dritten entgegen, kann sich auch ein Pseudonym aufgrund markenrechtlicher Vorschriften gegen die Verwendung durch einen Nichtberechtigten durchsetzen. Bei Gleichnamigkeit, wenn also zwei Personen mit dem Namen Anton Müller die E-Mail-Adresse anton.mueller @example.com registrieren wollen, gilt das Recht des Schnelleren. Wer ein Namensrecht hat und die entsprechende Adresse als Erster registriert, hat Glück. Solche Fälle kommen insbesondere im Bereich der E-Mail-Adressen von Webmail- und Freemail-Anbietern wie GMX vor.

Nach den allgemeinen Geschäftsbedingungen der meisten Internet-Provider sind die Nutzer für die Einhaltung der Gesetze – und damit auch der Vorschriften zum Namensrecht – verantwortlich. In den AGB von GMX heißt es hierzu etwa: „Die vom Kunden reservierten und/oder genutzten […] E-Mail-Adressen […] dürfen mit Form, Inhalt und Zweck nicht gegen gesetzliche Verbote/Gebote, Rechte Dritter oder die guten Sitten verstoßen“. Aber auch hier gelten die Vorschriften des Telemediengesetzes, wonach ISPs bei Kenntnis von Rechtsverstößen von fremden Informationen, „die sie für einen Nutzer speichern“, auf Unterlassung und in offensichtlichen Fällen auch auf Schadensersatz in Anspruch genommen werden können. Erhalten sie später Kenntnis, müssen sie „unverzüglich tätig werden“, um die rechtswidrige Informationen aus dem Netz zu nehmen. Dies umfasst auch die unter einer von einem ISP verwalteten Domain „geschalteten“ E-Mail-Adressen, die (Namens-)Rechte Dritter verletzen. Auch Provider müssen sich also mit den (namens-)rechtlichen Grenzen der E-Mail-Adressen auseinandersetzen und ein kritisches Auge darauf werfen, was „unter“ ihrer Domain alles läuft.

Was für Namen von Personen gilt, gilt selbstverständlich auch für markenrechtlich geschützte Bezeichnungen. Hat jemand eine Marke für sich schützen lassen, darf ein anderer grundsätzlich keine gleichlautende Domain auf sich registrieren, wenn das den Markenschutz beeinträchtigen würde. Das Gleiche gilt bei der Verwendung im Local Part von E-Mail-Adressen, wobei hier an die Behauptung der Beeinträchtigung von Interessen des Markeninhabers höhere Anforderungen gestellt werden müssen.

Generischen Begriffen und ihrer Verwendung in E-Mail-Adressen stehen selten juristische Bedenken gegenüber. E-Mail-Adressen nach den Role-Account-Mustern info@…, support@… oder postmaster@…, aber auch kon takt@… oder – trotz etwaiger abweichender Interessen der Deutschen Post AG beispielsweise – post@… sind grundsätzlich immer möglich.

Schutz vor Veröffentlichung

Auch in anderem Zusammenhang gibt es Gerichtsurteile, etwa zur Frage, wann Dritte E-Mail-Adressen veröffentlichen dürfen. Zwar enthalten geschäftliche E-Mail-Adressen häufig personenbezogene Daten der Adresseninhaber, denn häufig folgen diese dem Muster (vorname.)nachname@example.com. Die Tatsache, dass personenbezogene Daten im Spiel sind, die nach den Datenschutzgesetzen – und in Deutschland insbesondere nach dem Bundesdatenschutzgesetz – besonders geschützt sind, bedeutet aber noch lange nicht, dass Namensträger und E-Mail-Adresseninhaber einer Veröffentlichung ihrer E-Mail-Adressen auch stets widersprechen können.

Vor dem Verwaltungsgericht Neustadt unterlag 2007 ein Beamter in einer entsprechenden Klage gegen seinen Dienstherrn. Der hatte nicht nur den Namen des Beamten, sondern auch seine ihm zugewiesene – aus seinen Namensbestandteilen zusammengesetzte – dienstliche E-Mail-Adresse im Web veröffentlicht. Die Neustädter Richter kamen in ihrer Interessenabwägung zu dem Schluss, dass die Veröffentlichung von Mitarbeiterdaten in Geschäftsordnungs- oder Organisationsplänen sowie Telefonverzeichnissen einer Dienststelle aus organisatorischen Gründen grundsätzlich rechtlich zulässig sei. Nur wenn Belästigungen des Beamten drohen, könne ausnahmsweise eine Unterlassung der Veröffentlichung geboten sein, so das Gericht. Dem Beamten half auch nicht der Einwand, er habe gar keinen „regelmäßigen Publikumsverkehr“, sodass die Veröffentlichung gerade seiner personenbezogenen Daten gar nicht erforderlich sei. Dieses Urteil und die darin festgelegten Abwägungskriterien dürften auch bei der Veröffentlichung von E-Mail-Adressen durch nichtöffentliche Arbeitgeber gelten.

Fazit

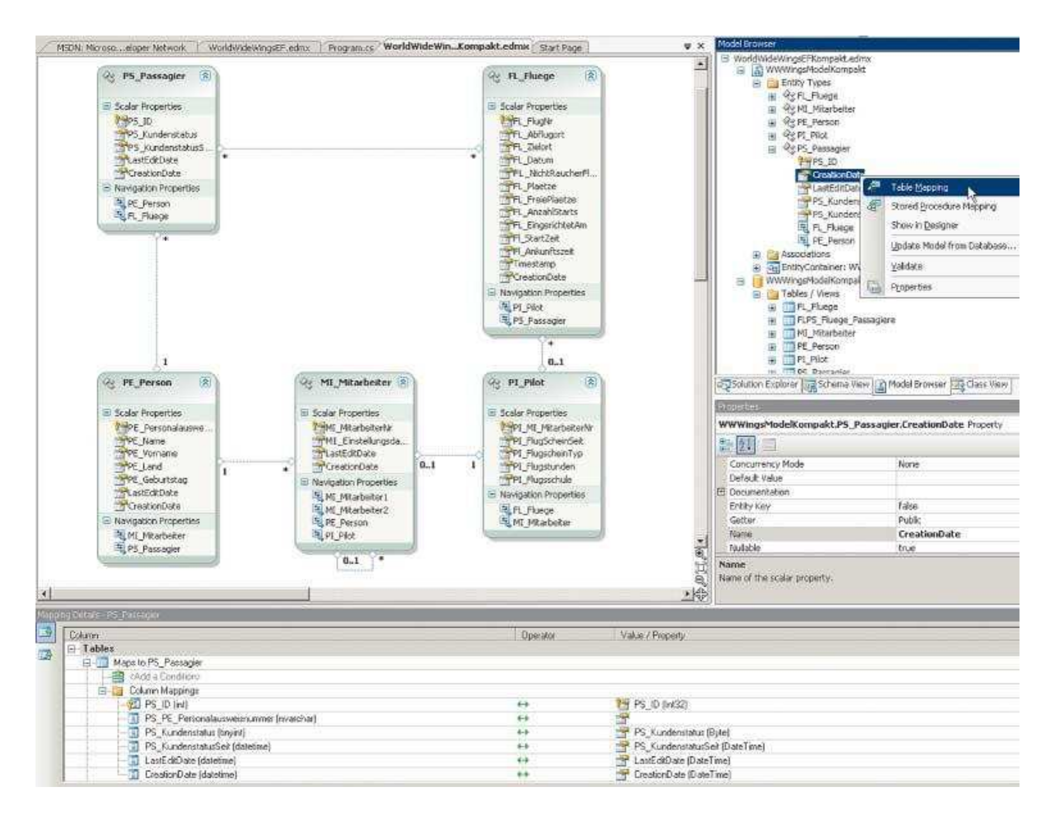
E-Mail-Adressen befinden sich nicht in einem rechtsfreien Raum. Zwar liegt ein Fokus und ein größeres Risiko bei der Verwendung von Bezeichnungen als Domains, die für Dritte geschützt sind, als bei einer Verwendung solcher Bezeichnungen im Local Part einer E-Mail-Adresse. Allerdings gibt es auch dort rechtliche Grenzen, die – insbesondere nach der Rechtsprechung des Bundesgerichtshofs – eine Interessenabwägung im Einzelfall erfordern. Grundsätzlich gilt die Rechtslage einer Domain auch für alle E-Mails mit dieser Domain-Bezeichnung nach dem „@“. Umgekehrt gilt dies aber nicht immer auch für die Verwendung einer solchen Bezeichnung im Local Part der Adresse. Hier ist abzuwägen.

Gegen die Veröffentlichung „seiner“ E-Mail-Adresse kann man dann keine Ansprüche geltend machen, wenn es sich um eine geschäftliche E-Mail-Adresse handelt und der Arbeitgeber ein schutzwürdiges Interesse an der Veröffentlichung hat. Das ist beispielsweise bei Behörden der Fall, die dem Bürger persönliche Kontaktmöglichkeiten im Internet zur Verfügung stellen und nicht lediglich unpersönliche E-Mail-Formulare verwenden wollen. Aber auch hier gilt natürlich, dass Unternehmen (aber auch Behörden) die schutzwürdigen Interessen ihrer Arbeitnehmer und Beamten berücksichtigen müssen. Hier geben auch die datenschutzrechtlichen Vorschriften entsprechende Wegweisungen. Im Zweifel haben die Interessen der Betroffenen am Schutz ihrer personenbezogenen Daten – wie Vor- und Nachname als Bestandteile einer E-Mail-Adresse – den Vorrang. Aber eben nur im Zweifel. (un)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.





.Net Framework 3.5 Service Pack 1

Verkappte Vier

Holger Schwichtenberg

Die kommenden Erweiterungen für .Net 3.5 nur als „Service Pack“ zu bezeichnen, ist eine Fehldeklaration. „Version 4.0“ wäre eine adäquate Bezeichnung, denn insbesondere in den Bereichen Datenzugriff und Webprogrammierung gibt es umfangreiche Neuerungen.

Das .Net Framework 3.5 war nur eine kleine Erweiterung im Vergleich zu den Vorgängerversionen: Während es für den Datenzugriff durch die Language Integrated Query (LINQ) noch eine weitreichende Verbesserung und für verteilte Systeme sowie Webservices nennenswerte Erweiterungen gab, gingen die Bereiche Desktop- und Webentwicklung fast leer aus. Man musste kein Insider sein, um zu merken, dass Microsoft viele einst für .Net 3.5 angekündigte Funktionen verschoben hatte. Das Ziel dieser Verschiebung ist aber nun nicht .Net 4.0, sondern das Service Pack 1 für .Net 3.5 – stringent und logisch ist das nicht.

OR-Mapper zum Zweiten

LINQ ist eine allgemeine Such- und Abfragesprache für unterschiedliche Datenspeicher (s. *iX*-Link [a]). Die entsprechende Variante für Datenbanken, LINQ-to-SQL, ist zugleich ein objektrelationaler Mapper (ORM), der Zeilen in Datenbanktabellen auf Objekte abbilden kann. Noch während der Entwicklung von LINQ-to-SQL hatte Microsoft angekündigt, einen zweiten ORM auf den Markt zu bringen, das ADO.Net Entity Framework (EF). EF ist – nun Bestandteil des Service Packs – keineswegs eine Weiterentwicklung von LINQ-to-SQL, sondern eine (ungewollte) Parallelentwicklung in Redmond. Die kuriose Geschichte des OR-Mapping bei Microsoft, die im Jahr 2003 mit dem nie erschienenen Werkzeugen Object Spaces und Windows File System (WinFS) begann, bekommt somit ein neues Kapitel.

LINQ-to-SQL und EF gleichen sich hinsichtlich der Verwendung von LINQ als primäre Abfragesprache; damit hört es aber fast schon mit den Gemeinsamkeiten auf (s. Tabelle „Unterschiede zwischen EF und LINQ-to-SQL“). Im Zentrum steht die größere Flexibilität des EF, da zum einen neben Microsofts SQL Server andere Datenbanken unterstützt werden und zum anderen flexiblere Abbildungsszenarien sowie komplexere Serialisierung möglich sind.

Aber LINQ-to-SQL hat auch Funktionen, die das EF noch nicht hat: Dazu gehört insbesondere das Forward Engineering, also die Generierung des kompletten Datenbankschemas aus bestehenden Geschäftsobjekten heraus (in der Java-Welt als „Container Managed Persistance“ bekannt). Auch beim transparenten Nachladen (Lazy Loading) kann LINQ-to-SQL punkten; beim EF muss der Entwickler ein explizites *Load()* absetzen, um abhängige Unterobjekte zu laden.

Die letzte Zeile in der Tabelle hat es in sich: Das EF verlangt eine Basisklasse für alle zu persistierenden Klassen. LINQ-to-SQL hat diese Anforderung nicht und bietet daher die in OO-Entwicklerkreisen geschätzten „POCOs“. POCO steht für Plain Old CLR Object und bezeichnet einige .Net-Klassen, an die es keine Anforderungen seitens der Infrastruktur gibt (z. B. eine Basisklasse oder eine Schnittstelle). POCOs sind groß im Kommen und daher unterstützt auch die Verteilungsplattform WCF (Windows Communication Foundation) ab Service Pack 1 POCOs bei der binären Serialisierung. Bisher konnte man POCOs nur nutzen, wenn man den XML-Serialisierer für Webservices verwendet hat.

EF ist intern wesentlich komplexer aufgebaut als LINQ-to-SQL. Microsoft setzt über den klassischen ADO.Net Data Provider zunächst einen speziellen Provider für das EF, der in der Lage ist, die verwendete datenbankneutrale Abfragesprache „Entity SQL“ (eSQL) in datenbankspezifische SQL-Befehle zu übersetzen (s. Grafik). Zudem arbeitet eSQL nicht auf dem relationalen Datenbankschema, sondern auf einer konzeptuellen Ebene, die man aus der Entity-Relationship-Modellierung (ERM) kennt. Im Gegensatz zum relationalen Modell gibt es hier zwischen Entitäten echte N:M-Beziehungen. Die Abbildung zwischen Tabellen in Entitäten erfolgt im Entity Data Model (EDM) in drei getrennten Beschreibungssprachen für Datenbankschema (SSDL), konzeptuelles Modell (CSDL) und Abbildung zwischen den beiden erstgenannten (MSL).

Die Vorteile von eSQL kann man einsetzen, ohne objektrelationales Mapping betreiben zu müssen, denn der sogenannte „EntityClient Data Provider“ bietet Zugang zu den Daten mit klassischen ADO.Net-Instrumenten wie *DataReader* und *DataSet* – allerdings nur lesend. Das eigentliche ORM erfolgt auf der Ebene der Object Services (hier auch schreibend). Durch die Object Services werden aus den Tabellen Objektmengen und auf dieser obersten Ebene kann man schließlich LINQ-to-Entities anwenden, um mit streng typisierten und vom Compiler zur Entwicklungszeit geprüften Abfragen auf die Datenbanken zuzugreifen.

Unterschiede zwischen EF und LINQ-to-SQL

	LINQ-to-SQL	ADO.Net Entity Framework
Verfügbarkeit	ab .Net 3.5	ab .Net 3.5 Service Pack 1
unterstützte Datenbank	nur Microsoft SQL Server, einschließlich Express- und Compact-Version	viele verschiedene Datenbanken, z. B. Microsoft SQL Server, Oracle, DB2, Informix, MySQL, Postgres, Ingres, Sybase sowie alle Datenbanken mit ODBC- oder JDBC-Treiber
Abbildungsszenarien	1:1-Mapping und Filtered Mapping für Vererbung	1:1, 1:N, M:N sowie Vererbung durch Filtered Mapping, vertical Mapping und horizontal Mapping
Abfragesprachen	LINQ, SQL	LINQ-to-Entities, eSQL
Abbildung auf Objektebene	ja	ja
Abbildung auf Tabellenebene	nein	ja
Reverse Engineering	ja	ja
Forward Engineering	nein	ja
Serialisierung	einfach	komplette Objektbäume
Nachladen von Objekten	transparent	nicht transparent
Designer-Dateien	*.dbml*	*.edmx*
Basisklasse für Geschäftsobjekte	keine („POCOs“, s. Text)	*System.Data.Objects.DataClasses.EntityObject*

Änderungen über Webservice

Eine ebenfalls mit dem Service Pack 1 eingeführte Spielart des EF sind die ADO.Net-Data-Services. Mit ihnen kann man eine Datenbank über einen Webservice auslesen und verändern. Natürlich war dies auch bisher möglich, indem man sich selbst einen solchen Webservice geschrieben hat. Neu ist, dass das .Net Framework eine Standardimplementierung enthält. Außerdem gibt es eine Funktion, die selbst nicht zu leicht zu erreichen wäre: Der Webservice lässt sich über LINQ ansprechen und versteht (fast) alle LINQ-Befehle. Während man bei einem eigenen Webservice etliche verschiedene Methoden implementieren muss und bei neuen Anwendungsfällen (z. B. einem neuen Filterkriterium) den Webservice erweitern musste (wenn man sich nicht die Mühe gemacht hatte, eine eigene Abfragesyntax im Webservice anzubieten), kann man nun vom Client aus per LINQ einen universellen, generischen Datendienst ansprechen.

Neues im Bereich ASP.Net

Auf der Serverseite muss der Entwickler dazu lediglich ein EF-Modell der Datenbank sowie eine WCF-Dienstdatei (*.svc*) bereitstellen. Erstes schafft ein Assistent in Visual Studio 2008 mit Service Pack 1, Letzteres der Entwickler in drei Codezeilen. Der Client bekommt einen durch *DataSvcUtil.exe* generierten Proxy und greift damit auf das entfernte EF-Modell zu, als wäre es lokal vorhanden. Einziger Wermutstropfen: Die Kommunikation erfolgt im REST-basierten Stil mit Serialisierung in den Formaten *ATOM* und *JSON*, einen SOAP-Webservice kann man damit nicht bauen.

ASP.Net-Entwickler konnten sich am .Net Framework 3.5 nicht so recht erfreuen, denn die Änderungen gegenüber der 2.0-Version waren bescheiden im Vergleich zu den großen Ankündigungen, die Microsoft in Vorabprodukten wie „Atlas“ und den „ASP.Net Futures“ gezeigt hatte. Mit dem Service Pack 1 kommt einiges von diesen Ankündigungen tatsächlich ins Produkt. An erster Stelle stehen hier die ASP.Net-Dynamic-Data-Controls zum Aufbau datengetriebener Websites nach dem Prinzip des Rapid Application Development (RAD).

Klassisch hat man eine Website-Oberfläche für die Datennavigation/-manipulation entwickelt und anschließend an eine Datenquelle gebunden. Bei den Dynamic Data Controls generiert sich die Oberfläche aus den Daten zunächst selbst, einschließlich Navigation zwischen den Tabellen und Datenmasken zur Veränderung der Daten. Der Webentwickler kann durch Konfigurationseinstellungen oder eigene Vorlagen die Ausgabe noch in gewissen Grenzen modifizieren. Dynamic Data Controls sind somit kein Instrument für Entwickler, die volle Kontrolle haben wollen, sondern für die, die eine 90 %-Lösung verlangen, die schnell fertig ist.

Das Gegenstück für Puristen und Enterprise-Architekten wäre das Modell View Controller Framework für ASP.Net. Allerdings hat Microsoft dies aus dem Service

iX-TRACT

- Service Pack 1 für .Net Framework 3.5 enthält weitreichende Erweiterungen.
- Neben dem bereits mit Version 3.5 eingeführten LINQ-to-SQL gibt es nun einen weiteren objektrelationalen Mapper: das ADO.Net Entity Framework.
- ASP.Net-Dynamic-Data-Controls unterstützen den Aufbau datengetriebener Websites.
- Das monolithische .Net Framework Redistributable ist in einer zweiten Form von reinen „Serverklassen“ befreit und damit auch in einer abgespeckten Client-Version verfügbar.

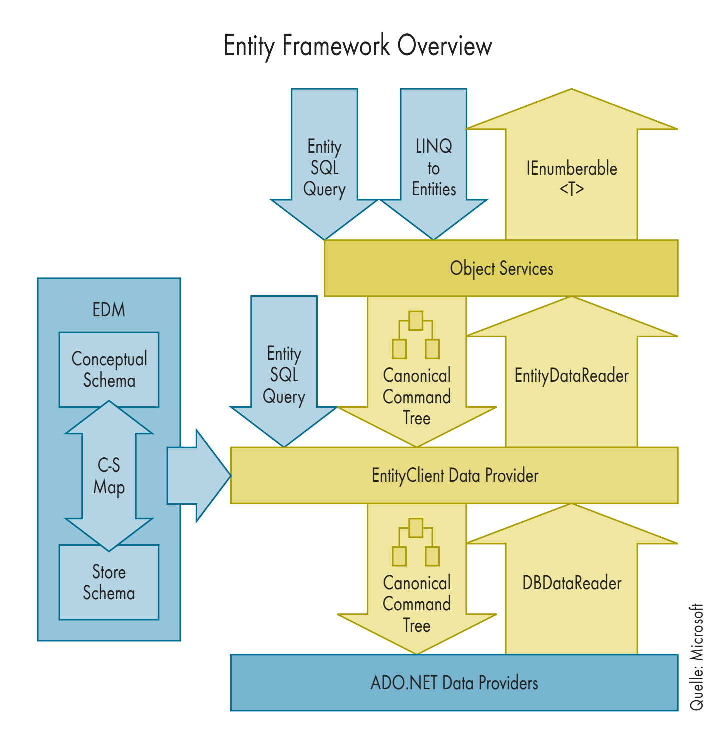
Pack 1 ausgelagert und bietet es als Erweiterung (auch im Quellcode) an [b]. Dringebliebe n sind aber weitere interessante Punkte für Webentwickler. Hervorzuheben ist die Unterstützung für die Browser-Historie in AJAX-Seiten, das Kombinieren von Javascript-Dateien, die bessere Unterstützung für URL-Rewriting sowie die Unterstützung des Einbettens von Silverlight-Inhalten in ASP.Net-basierten Webseiten und die Datenbindung an EF-Modelle. Entwickler, die sich für Vorabversionen begeistern können, finden unter [b] zudem noch das nächste ASP.Net 4.0, mit dem clientseitige Datenbindung in Javascript möglich wird.

Framework für Arbeitsplatzrechner

Im Prinzip längst überfällig: Microsoft hat nun damit begonnen, das monolithische .Net Framework Redistributable in fallspezifische Teilmengen aufzubrechen. Bisher wurden auch rein serverseitige Bibliotheken auf jedem Rechner installiert, selbst wenn er als Arbeitsplatzrechner diese Funktionen nicht benötigt. Mit dem „.Net Framework Client Profile“ gibt es jetzt eine abgespeckte Variante des .Net Framework, die auf alle Bibliotheken verzichtet, die (üblicherweise) nur in Serveranwendungen Verwendung finden (z. B. ASP.Net, Workflow und WCF).

Visual Studio 2008 unterstützt ab Service Pack 1 die Kompilierung gegen das Client Profile. Die Entwicklungsumgebung warnt den Entwickler, wenn er Bibliotheken verwendet, die nicht zu dessen Spektrum gehören. Zur Laufzeit erhält ein Nutzer, der nur das Client Profile installiert hat und eine Anwendung startet, die mehr Bibliotheken erfordert, die Chance, ein Upgrade auf das vollständige .Net Framework durchzuführen.

Neben dieser grundsätzlichen Änderung liefern die Redmonder mit dem Service Pack 1 neue Steuerelemente für WPF und für Windows Forms. Die dringend von den WPF-Entwicklern ersehnten Steuerelemente *DataGrid* und *DateTimePicker* gibt es aber auch dort nicht. Microsoft hat allerdings angekündigt [c], diese noch vor der Fertigstellung der 4.0-Version auszuliefern. Inzwischen können sich WPF-Entwickler über Verbesserungen bei der Datenbindung, den Überblendungseffekten und der Arbeit mit Nicht-Vektorgrafiken (Bitmaps) freuen. Außerdem will Microsoft die Start- und Ausführungsgeschwindigkeit von WPF-Anwendungen verbessert haben.



Die Schichten des ADO.Net Entity Framework

Fazit

Service Pack 1 für .Net 3.5 ist ein Muss für jeden Entwickler, denn es ist, wie eingangs gesagt, eigentlich die nächste Hauptversion. Microsoft wird aber noch einige Arbeit damit haben, Entwicklern den Unterschied zwischen LINQ-to-SQL und Entity Framework nahezubringen. Diese Konkurrenz im eigenen Haus ist nicht nachvollziehbar. (WM)

DR. HOLGER SCHWICHTENBERG

unterstützt mit seiner Firma www.IT-Visions.de Unternehmen beim Einsatz von Windows-Technologien. Er hält Vorträge auf Fachkonferenzen und ist Autor zahlreicher Fachbücher.

iX-Link ix0809108



Visual Studio 2008 Service Pack 1

Zusammen mit dem ersten Service Pack für das .Net Framework 3.5 bekommt auch Visual Studio 2008 ein Service Pack verpasst [d]. Neben zahlreichen Fehlerkorrekturen (z. B. die langsame Ladezeit des Webdesigners und Darstellungsprobleme im WPF-Designer) liefert Microsoft zahlreiche Ergänzungen:

– Im Bereich des Datenbankzugriffs gibt es einen Designer für EF-Modelle sowie Unterstützung für Microsofts SQL Server 2008 (s. Aufmacher).

– Für die Arbeit mit XML-Schemata wurde ein XML-Schema-Explorer eingeführt, der eine hierarchische Sicht des Aufbaus liefert.

– Für WCF gibt es eine Verbesserung des Testclients, eine Funktion zum Umbenennen, die die Konfigurationsdateien mit berücksichtigt, sowie einen kleinen Assistenten, der einen webbasierten WCF-Host generiert.

– C++ bekommt eine Erweiterung der Microsoft Foundation Classes (MFC) sowie eine Implementierung der unter dem Namen „Technical Report 1“ bekannten Klassen [e].

– Im Webdesigner lässt sich Javascript-Quellcode jetzt automatisch formatieren. Es gibt neue Vorlagen für die Implementierung von Modulen und Handlern für IIS 7.0.

– Der C#-Codeeditor zeigt nun bereits vor dem Kompilieren Eingabefehler an (wie schon für VB seit dem VS 2002).

– Der WPF-Designer enthält jetzt für jedes Steuerelement auch die aus Windows Forms bekannte Registerkarte für die Ereignisbindung. Außerdem wurde die Darstellung einiger Steuerelemente verbessert und das Drag & Drop von Steuerelementen aus der Werkzeugleiste in der XAML-Ansicht sowie das Sortieren im Eigenschaftsfenster hinzugefügt.

– Bei der Versionskontrolle wurde die Migration von Visual Source Safe auf Team Foundation Version Control verbessert.

– Für die Verbreitung gibt es mehr Optionen beim Click-Once-Deployment sowie Unterstützung für die Beschränkung auf das .Net Client Profile.

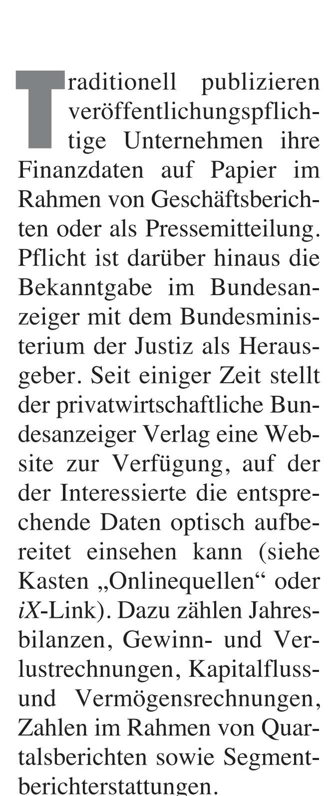
Finanzdaten-Kommunikation per XBRL

Transparente Firmen



Michael Härtfelder

Oftmals vergeblich sucht man im Web Finanzdaten von veröffentlichungspflichtigen Unternehmen. Ein Reporting-Standard sowie das ab Anfang dieses Jahres verpflichtende XBRL sollen die digitale Bekanntmachung erleichtern.



Traditionell publizieren veröffentlichungspflichtige Unternehmen ihre Finanzdaten auf Papier im Rahmen von Geschäftsberichten oder als Pressemitteilung. Pflicht ist darüber hinaus die Bekanntgabe im Bundesanzeiger mit dem Bundesministerium der Justiz als Herausgeber. Seit einiger Zeit stellt der privatwirtschaftliche Bundesanzeiger Verlag eine Website zur Verfügung, auf der der Interessierte die entsprechende Daten optisch aufbereitet einsehen kann (siehe Kasten „Onlinequellen“ oder *iX*-Link). Dazu zählen Jahresbilanzen, Gewinn- und Verlustrechnungen, Kapitalfluss- und Vermögensrechnungen, Zahlen im Rahmen von Quartalsberichten sowie Segmentberichterstattungen.

Unmittelbar lässt sich darauf jedoch nicht zugreifen. Bei direktem Zugriff müssten die Konsumenten die Daten nicht länger manuell in ihre Systeme eintippen oder dafür kostenpflichtige Dienste von Finanzdienstleistern in Anspruch nehmen. Geschwindigkeitsgewinne ließen sich ebenfalls erzielen: Veröffentlicht etwa die Deutsche Lufthansa in einem Quartalsbericht einen deutlich unter den Erwartungen liegenden Gewinn, stünde diese Information dem Publikum sofort zur Verfügung. Verteilen ließen sich die digitalisierten Daten beispielsweise über einen RSS-Feed.

Alles in Harmonie

Über eine Analysesoftware ließe sich die frische Information unmittelbar auswerten. Zeitlich oder räumlich näher an der Quelle angesiedelte Benutzer könnten diese Tatsache nicht mehr als Vorteil ausspielen.

Obwohl Rechnungslegung und Finanzberichterstattung in den verschiedenen Ländern auf nationalen Richtlinien und Gesetzen beruhen, lässt sich ein deutlicher Trend hin zu einem harmonisierten Geschäfts-Reporting ausmachen. Die globalisierten Kapitalmärkte fordern vergleichbare Jahresabschlüsse und Finanzdaten unabhängig vom Land, in dem sie publiziert werden. Schon seit vielen Jahren beschäftigen sich Gremien mit der Formulierung eines international anerkannten Rechnungslegungsstandards: IFRS (International Financial Reporting Standards) soll die nationalen Regelungen (etwa HGB in Deutschland oder US-GAAP in den USA) ersetzen. Regierungen, Börsen und Wirtschaftsprüfungsgesellschaften unterstützen diese Bemühungen.

Die dazu passende technische Spezifikation zur Abfassung der notwendigen elektronischen Dokumente heißt XBRL (Extensible Business Reporting Language) und ist ein lizenzfrei nutzbares XML-Derivat [1]. Die Federführung liegt bei XBRL International, einem Zusammenschluss von weltweit rund 550 Unternehmen. Seit dem 1. Januar 2008 sind deutsche börsennotierte Unternehmen gesetzlich dazu verpflichtet, ihre Finanzdaten in diesem Format zu veröffentlichen. Einige Rechnungswesenprogramme, etwa von SAP, können XBRL-Dokumente aus Datenbanken generieren. Ob komplexe Strukturen sowie Konformitätsvorschriften dabei korrekt abgebildet werden, entzieht sich leider der einfachen Überprüfbarkeit.

Um das enorme Potenzial von XBRL erahnen zu können, muss man sich dessen ungewöhnliche Position in der Softwarewelt vor Augen halten: Während im Allgemeinen zuerst die Software (etwa Ruby, Groovy, Ajax, Phyton) entsteht und dann in der Welt nach Anhängerschaft sucht, ist es bei XBRL genau andersherum. Hier fand das Konzept eine große weltweite Anhängerschaft, die bezahlbaren und flexiblen Softwareprodukte werden noch gesucht.

Hinzu kommt, dass der Erfolg von XBRL eng an die Einführung von IFRS gekoppelt ist. Wie bei jedem komplexen internationalen Abstimmungsprozess nahm die Synchronisation der Vorstellungen Jahre in Anspruch.

iX-TRACT

- Ab Anfang dieses Jahres müssen deutsche börsennotierte Unternehmen ihre Finanzdaten nach dem XBRL-Standard im Web offenlegen.
- XBRL schafft gegenüber der Papiervariante zahlreiche Vorteile, beispielsweise lassen sich die Daten direkt auswerten.
- Der Wille der EU, die Finanzmärkte durchsichtiger zu gestalten, eröffnet einen Markt für XBRL-Anwendungen.

Das Warten hat sich jedoch gelohnt, die betroffenen Firmen können die XBRL-Taxonomien verlässlich erstellen. Dies wiederum schafft die Voraussetzung dafür, dass sich die zunächst unverbindlichen Empfehlungen in verbindliche Verordnungen umwandeln lassen.

Prinzipiell enthält eine XBRL-Architektur zwei Komponenten: Instanzdokumente sowie die referenzierte Taxonomie. Während das Instanzdokument konkrete Daten und Fakten eines Unternehmen bereitstellt, legt die Taxonomie fest, wie dies technisch und organisatorisch auszusehen hat. Instanzdokument und Taxonomie verhalten sich zueinander wie ein XML-Dokument zum dazugehörigen XML-Schema (XSD, XML Schema Definition). Vereinfacht formuliert entspricht eine Taxonomie einem Rechnungslegungswerk. Es gibt eine Taxonomie für den IFRS, eine für das HGB, eine für die US-GAAP et cetera.

Berichte mit Struktur

Technisch gesehen bestehen Taxonomien aus einer Sammlung abhängiger XML-Schemas, die wiederum andere XSDs referenzieren können. Hinterlegt sind hier die Anordnung der Daten, die maximal möglichen Elemente in den XBRL-Instanzdokumenten sowie deren Beziehungen untereinander. Jedes Instanzdokument bezieht sich auf genau eine Taxonomie. In der Praxis erstellen die Entwickler neue Taxonomien aus schon vorhandenen, die sie für ihre Zwecke anpassen. Eine Auswahl allgemeiner Taxonomien liegt auf der Homepage der XBRL-Organisation. Die Gesamtheit aller für ein Instanzdokument maßgeblichen XSDs und Linkbases (dazu später mehr) heißt DTS (Discoverable Taxonomy Set). Eine detaillierte Beispieltaxonomie sowie die dazugehörigen Instanzdokumente liegen auf dem *iX*-FTP-Server (siehe *iX*-Link am Ende des Textes).

Konkret könnten in einem solchen Dokument Positionen eines Geschäftsberichts stehen (etwa „Basic Earnings (Loss) Per Share“). Einzelwerte ohne strukturellen Aufbau heißen *item*, zusammengehörige *tuple*. Ein Tuple kann Items oder andere Tuples enthalten. Jedes Item (als atomare Einheit) repräsentiert ein Business Concept, das heißt, einen speziellen Sachverhalt, der im Detail in der dazugehörigen Taxonomie definiert ist. Weiterhin muss jedes Item in einem festgelegten Kontext interpretiert werden. Das könnte beispielsweise die referenzierte Zeitperiode (Jahr 2004, III Quartal) oder die Berichtskategorie (Vergangenheit, Planung, nicht konsolidiert) sein.

XBRL-Instanzen und Taxonomien können optional sogenannte Linkbases referenzieren. Die enthalten zusätzliche Informationen zu den in einer Instanz aufgeführten Fakten beziehungsweise beschreiben Beziehungen zwischen ihnen. Dieses Zusammenhänge legt der Entwickler mithilfe der XML-Spracherweiterung XLink (XML Linking Language) an. Ähnlich wie Hyperlinks auf Webseiten bieten XLinks die Möglichkeit, Komponenten miteinander zu verbinden und mit zusätzlichen Attributen zu versehen. XLinks sind mehr als einfache textuelle Verbindungen, da sie selbst Metadaten, etwa Hierarchieinformationen, enthalten. Linkbases gehören als Bestandteil zum DTS. Sie bieten fünf Arten von Links: Label, Reference, Calculation, Definition, Presentation.

Label Links verbinden einzelne Fakten mit einer offiziellen Bezeichnung. Jedes Berichtselement kann Links zu verschiedenen Labels haben. Dies ist zum Beispiel der Fall, wenn ein Report in mehreren Sprachen veröffentlicht werden soll. Listing 1 ordnet dem Business Concept *ifrs-gp _AmountMaximumPotential-*

Listing 1: Label Links

```
<labelLink      xlink:type="extended"
                xlink:role="http://www.xbrl.org/2003/role/link">
  <loc          xlink:type="locator"
                xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_AmountMaximumPotentialLossFromCreditRisk"
                xlink:label="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk" />
  <labelArc     xlink:type="arc"
                xlink:arcrole="http://www.xbrl.org/2003/arcrole/concept-label"
                xlink:from="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk"
                xlink:to="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk_lbl" />
  <label        xlink:type="resource"
                xlink:role="http://www.xbrl.org/2003/role/label"
                xlink:label="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk_lbl"
                xml:lang="en">Amount of Maximum Potential Loss from Credit Risk</label>
  ...
</labelLink>
```

Listing 2: Reference Links

```
<referenceLink  xlink:type="extended"
                xlink:role="http://www.xbrl.org/2003/role/link">
  <loc          xlink:type="locator"
                xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_AmountMaximumPotentialLossFromCreditRisk"
                xlink:label="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk" />
  <referenceArc xlink:type="arc"
                xlink:arcrole="http://www.xbrl.org/2003/arcrole/concept-reference"
                xlink:from="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk"
                xlink:to="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk_ref" />
  <reference    xlink:type="resource"
                xlink:role="http://www.xbrl.org/2003/role/reference"
                xlink:label="ifrs-gp_AmountMaximumPotentialLossFromCreditRisk_ref">
    <ref:Name>IAS</ref:Name>
    <ref:Number>32</ref:Number>
    <ref:Paragraph>66</ref:Paragraph>
  </reference>
  ...
</referenceLink>
```

Listing 3: Calculation Links

```
<calculationLink  xlink:type="extended"
                  xlink:role="http://xbrl.iasb.org/int/fr/ifrs/gp/role/BalanceSheetLiquidity"
                  xlink:title="Balance Sheet, Order of Liquidity Format">
  <loc            xlink:type="locator"
                  xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_AssetsTotal"
                  xlink:label="ifrs-gp_AssetsTotal" />
  <loc            xlink:type="locator"
                  xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_PropertyPlantEquipmentNet"
                  xlink:label="ifrs-gp_PropertyPlantEquipmentNet" />
  <calculationArc xlink:type="arc"
                  xlink:arcrole="http://www.xbrl.org/2003/arcrole/summation-item"
                  xlink:from="ifrs-gp_AssetsTotal"
                  xlink:to="ifrs-gp_PropertyPlantEquipmentNet" order="1" weight="1" use="optional" />
  <loc            xlink:type="locator"
                  xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_InvestmentProperty"
                  xlink:label="ifrs-gp_InvestmentProperty" />
  <calculationArc xlink:type="arc"
                  xlink:arcrole="http://www.xbrl.org/2003/arcrole/summation-item"
                  xlink:from="ifrs-gp_AssetsTotal"
                  xlink:to="ifrs-gp_InvestmentProperty" order="2" weight="1" use="optional" />
  <loc            xlink:type="locator"
                  xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_IntangibleAssetsNet"
                  xlink:label="ifrs-gp_IntangibleAssetsNet" />
  <calculationArc xlink:type="arc"
                  xlink:arcrole="http://www.xbrl.org/2003/arcrole/summation-item"
                  xlink:from="ifrs-gp_AssetsTotal"
                  xlink:to="ifrs-gp_IntangibleAssetsNet" order="3" weight="1" use="optional" />
  ...
<calculationLink>
```

Onlinequellen

XBRL International
www.xbrl.org

XBRL Deutschland
www.xbrl.de

elektronischer Bundesanzeiger
www.ebundesanzeiger.de

zentrale Plattform zum Speichern von Unternehmensdaten
www.unternehmensregister.de

allgemeine Taxonomien
www.xbrl.org/FRTaxonomies/

ABRA-Projekt
www.xbrlopen.org

LossFromCreditRisk aus der Taxonomie *ifrs-gp-2004-06-15.xsd* das Label (hier nur auf Englisch) „Amount of Maximum Potential Loss from Credit Risk“ zu.

In ähnlicher Weise stellen Reference Links eine Verbindung her zwischen einzelnen Fakten und den zugrunde liegenden Stellen in Rechtsverordnungen. Listing 2 nimmt mit *ifrs-gp_AmountMaximumPotentialLossFromCreditRisk* aus der Taxonomie *ifrs-gp-2004-06-15.xsd* Bezug auf die Rechnungslegungsvorschrift IAS 32, Paragraf 66.

Während die beiden bisher dargestellten Link-Typen auf externe Quellen verweisen, verbinden die übrigen drei Elemente untereinander. Calculation Links legen fest, wie sich einzelne Daten aus anderen Daten berechnen lassen. Eines der Attribute (*weight*) ist das Gewicht, mit dem ein Ausgangswert in den Zielwert einfließt. Listing 3 berechnet den Wert von *ifrs-gp_AssetsTotal* in der Taxonomie *ifrs-gp-2004-06-15.xsd* aus der Summe der einfachen (*weight =“1“*) Werte von *ifrs-gp_PropertyPlantEquipmentNet*, *ifrs-gp_InvestmentProperty*, *ifrs-gp_IntangibleAssetsNet* plus eventuell weiteren.

Klarheit in den Finanzen

XBRL ist zunächst einmal ein elektronischer Behälter für den Transport von Finanzdaten. Zusätzlich soll er die Möglichkeit bieten, aus einer XBRL-Instanz einen schriftlichen Report zu generieren. Die bisher erwähnten Konstrukte geben Hinweise auf die Struktur eines Geschäftsberichtes. Hier kommen die Presentation Links ins Spiel, sie beschreiben die Darstellungshierarchie der einzelnen Elemente. Beispielhaft zeigt Listing 4, wie die Felder *ifrs-gp_PropertyPlantEquipmentNet*, *ifrs-gp_InvestmentProperty*, *ifrs-gp_IntangibleAssetsNet* (und zwar in genau dieser Reihenfolge, *order=“1,2,3“*) dem Feld *ifrs-gp_AssetsPresentation* und dieses wiederum dem Feld *ifrs-gp_BalanceSheetPresentation* in einer schriftlichen Präsentation untergeordnet werden.

Definition Links legen Verallgemeinerungen und Spezialisierungen innerhalb der deklarierten Elemente fest. Eine Beziehung beziehungsweise Rolle zwischen zwei Elementen nennt sich *arcrole*. Entsprechend der *arcrole* (*parent-child* oder *child-parent*) existieren wechselseitige Beziehungen zwischen den Feldern (Listing 5).

Man sollte annehmen, dass sich die XML- und XSD-Dateien eines XBRL-Systems mit XSLT bearbeiten lassen. Aus Performancegründen setzen viele verfügbare Produkte jedoch für diesen Zweck auf Java oder eine andere Programmiersprache. Eine Ausnahme bildet das ursprünglich als Open Source gestartete ABRA-Projekt (Adaptive Business Reporting Automat). Dort basiert die gesamte Verarbeitung auf XSLT. Gut strukturiert bildet das Werkzeug für die Entwicklung von Reporting-Anwendungen XBRL-Funktionen mit XSLT-Bibliotheken nach. Leider hapert es noch in der Praxis: Die letzte frei verfügbare Version 0.9.1 ließ sich nicht zum Laufen bringen. Alle folgenden Versionen sind nur noch kostenpflichtig zu beziehen.

Das lässt sich jedoch verschmerzen, denn die überwiegende Mehrheit der zumeist mittelständischen Unternehmen reicht ihre Abschlüsse ohnehin bei der Datev in Nürnberg ein und lässt diese die XBRL-Dateien generieren. Der Finanzdienstleister leitet die erstellten Dokumente wiederum an den Quasi-Monopolisten „elektronischer Bundesanzeiger“ weiter, der sie optisch aufbereitet auf seinen Webseiten zur Verfügung stellt. Ein Zugriff beziehungsweise die Veröffentlichung der Original-XBRL-Dokumente für die Öffentlichkeit ist derzeit nicht vorgesehen.

Listing 4: Presentation Links

```
<presentationLink  xlink:type="extended"
                   xlink:role="http://xbrl.iasb.org/int/fr/ifrs/gp/role/BalanceSheetLiquidity"
                   xlink:title="Balance Sheet, Order of Liquidity Format">
   <loc            xlink:type="locator"
                   xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_BalanceSheetPresentation"
                   xlink:label="ifrs-gp_BalanceSheetPresentation" />
   <loc            xlink:type="locator"
                   xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_AssetsPresentation"
                   xlink:label="ifrs-gp_AssetsPresentation" />
   <presentationArc xlink:type="arc"
                   xlink:arcrole="http://www.xbrl.org/2003/arcrole/parent-child"
                   xlink:from="ifrs-gp_BalanceSheetPresentation"
                   xlink:to="ifrs-gp_AssetsPresentation" order="1" use="optional" />
   <loc            xlink:type="locator"
                   xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_PropertyPlantEquipmentNet"
                   xlink:label="ifrs-gp_PropertyPlantEquipmentNet" />
   <presentationArc xlink:type="arc"
                   xlink:arcrole="http://www.xbrl.org/2003/arcrole/parent-child"
                   xlink:from="ifrs-gp_AssetsPresentation"
                   xlink:to="ifrs-gp_PropertyPlantEquipmentNet" order="1" use="optional" />
   <loc            xlink:type="locator"
                   xlink:href="ifrs-gp-2004-06-15.xsd#ifrs-gp_InvestmentProperty"
                   xlink:label="ifrs-gp_InvestmentProperty" />
   <presentationArc xlink:type="arc"
                   xlink:arcrole="http://www.xbrl.org/2003/arcrole/parent-child"
                   xlink:from="ifrs-gp_AssetsPresentation"
                   xlink:to="ifrs-gp_InvestmentProperty" order="2" use="optional" />
  ...
 <presentationLink>
```

Listing 5: Definition Links

```
<definitionLink    xlink:type="extended">
   <loc            xlink:type="locator"
                   xlink:href="ifrs-ci-2003-07-15.xsd#ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:label="ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:title="ifrs-ci_PropertyPlantEquipmentNet" />
   <definitionArc  xlink:type="arc"
                   xlink:from="ifrs-ci_BuildingsNetEndingBalance"
                   xlink:to="ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:show="replace"
                   xlink:actuate="onRequest"
                   xlink:title="Go up to: BuildingsNetEndingBalance"
                   xlink:arcrole="http://www.xbrl.org/linkprops/arc/child-parent" use="optional" />
   <definitionArc  xlink:type="arc"
                   xlink:from="ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:to="ifrs-ci_BuildingsNetEndingBalance"
                   xlink:show="replace"
                   xlink:actuate="onRequest"
                   xlink:title="Go down to: BuildingsNetEndingBalance"
                   xlink:arcrole="http://www.xbrl.org/linkprops/arc/parent-child" use="optional" />
   <definitionArc  xlink:type="arc"
                   xlink:from="ifrs-ci_FixturesFittingsNetEndingBalance"
                   xlink:to="ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:show="replace"
                   xlink:actuate="onRequest"
                   xlink:title="Go up to: FixturesFittingsNetEndingBalance"
                   xlink:arcrole="http://www.xbrl.org/linkprops/arc/child-parent" use="optional" />
   <definitionArc  xlink:type="arc"
                   xlink:from="ifrs-ci_PropertyPlantEquipmentNet"
                   xlink:to="ifrs-ci_FixturesFittingsNetEndingBalance"
                   xlink:show="replace"
                   xlink:actuate="onRequest"
                   xlink:title="Go down to: FixturesFittingsNetEndingBalance"
                   xlink:arcrole="http://www.xbrl.org/linkprops/arc/parent-child" use="optional" />
  ...
 </definitionLink>
```

Diese restriktive Handhabung ist durchaus gewollt. Frei verfügbare XBRL-Dokumente kollidieren mit den Geschäftsinteressen der etablierten Datenlieferanten wie Reuters, Vwd oder Bloomberg mit ihren teilweise proprietären Datenformaten. Maßnahmen wie die EU-Richtlinie zum Anlegerschutz (MiFID, Markets in Financial Instruments Directive) zeigen jedoch, dass der Wille besteht, die Finanzmärkte deutlich transparenter zu gestalten. Es ist absehbar, dass in Zukunft XBRL-Dokumente im Original zugänglich sein werden. Damit entstünde ein Markt für interessante Anwendungen auf Basis von XBRL. (jd)

MICHAEL HÄRTFELDER

arbeitet als selbstständiger Unternehmensberater in Frankfurt/Main im Banken- und Finanzdienstleistungsbereich.





Medizinische Software: Komplex und problembehaftet

Genormte Gesundheit

Christian Johner

Röntgenapparate oder Bestrahlungsgeräte müssen den strengen Anforderungen an ein Medizinprodukt genügen. Schließlich möchte niemand den Risiken fehlerhafter Technik ausgesetzt sein, schon gar nicht als Patient. Doch wie sieht es mit „medizinischer“ Software aus? Für deren Entwickler und Betreiber hat diese Klassifizierung weitreichende Konsequenzen.

Software arbeitet heute nicht nur als eingebetteter Bestandteil von Medizingeräten. Es gibt im medizinischen Umfeld zahlreiche eigenständig laufende Anwendungen sowie solche, die Medizingeräte steuern oder beeinflussen. Im gleichen Maße, wie sich medizinische Software verbreitet, vergrößern sich die damit verbundenen Probleme: Es vergeht keine Woche, in der das Bundesamt für Arzneimittel und Medizinprodukte (BfArM) keine softwarebedingten Fehler auf seiner Website veröffentlicht. So warnen Hersteller vor dem Speichern falscher Medikamentendosen, vor Daten, die verloren gehen, vor Fehldiagnosen bei EKGs und falschen Zuordnungen von Daten zu Patienten. Dabei dokumentieren die BfArM-Seiten nur die Fehler, die von bereits als Medizinprodukt klassifizierten Anwendungen stammen (siehe Kasten „Onlinequellen und *iX*-Link).

Sogenannte benannte Stellen – das können der TÜV oder andere staatlich akkreditierte Institutionen sein – betrachten ein eigenständig laufendes Programm unter gewissen Voraussetzungen als Medizinprodukt: Wenn es ein Medizingerät steuert oder beeinflusst (etwa Software zur Planung und Simulation von Bestrahlungen) oder wenn ein Gesetz dies explizit vorsieht. Auch wenn die Anwendung die Daten eines Medizingerätes analysiert (beispielsweise bei der Auswertung von Langzeit-EKG-Signalen) gehört sie in diese Kategorie. Ebenso wenn sie Diagnose oder Behandlung unterstützt (zum Beispiel Applikationen zur Diagnose des Aufmerksamkeitsdefizitsyndroms).

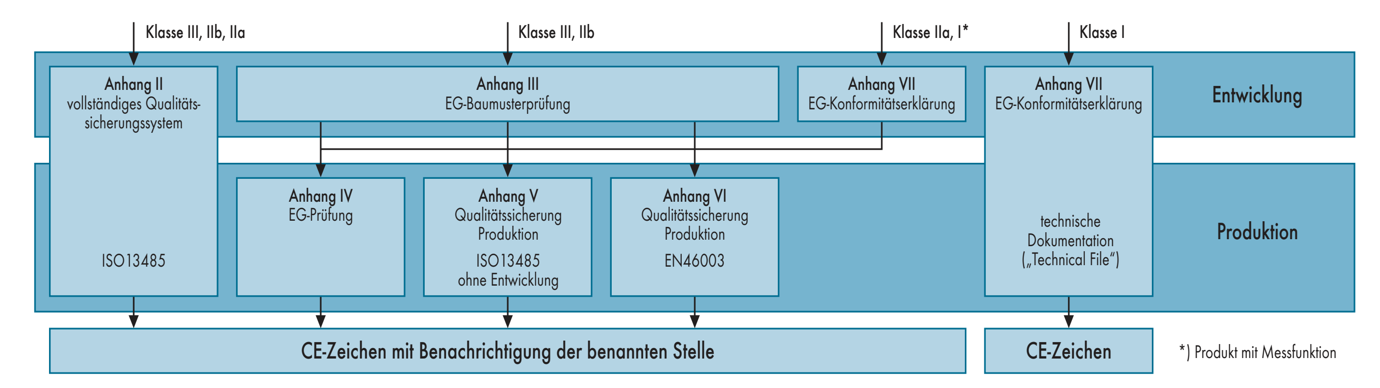
Heilen durch Software

Die europäische Medizinprodukte-Richtlinie 93/42/EC stellt in ihrer überarbeiteten Version vom November 2007 ebenfalls explizit klar, dass Software ein Medizinprodukt sein kann. Ein Gegenstand oder eine Software fällt in diese Kategorie, wenn er oder sie „vom Hersteller zur Anwendung für Menschen mittels ihrer Funktionen zum Zwecke der Erkennung, Überwachung, Behandlung und Linderung von Krankheiten und Verletzungen zu dienen bestimmt“ ist. Krankenhausinformationssysteme (KIS) gehören demnach nicht dazu. Sobald sie allerdings Module enthalten, die beispielsweise der Diagnose dienen, gar Expertenfunktionen, ändert sich das. Daher wird ein großer deutscher Hersteller sein neues KIS als Medizinprodukt auf den Markt bringen.

Einige Beispiele für medizinische Software [1]: Anwendungen zum Steuern, Überwachen sowie zur Parameteranzeige eines aktiven Medizinprodukts, etwa Spritzenpumpen, Beatmungs- oder Durchleuchtungsgeräte. Oder auch Programme für intensivmedizinische Monitoranlagen sowie solche zum Weiterleiten digitaler Patientenbilddaten auf Auswerte- und Befundungskonsolen zur Diagnostik (Stichwort Teleradiologie).

iX-TRACT

- Software, die medizinische Geräte steuert, sowie eigenständige Anwendungen im klinischen Umfeld unterliegen besonderen Sicherheitsanforderungen.
- Die Einstufung von Software als Medizinprodukt hat für Unternehmen spürbare Folgen, sie müssen beispielsweise den Herstellungsprozess daran ausrichten und genau dokumentieren.
- Medizinische Software ist trotz der zahlreichen Normen und Vorschriften oft fehlerhaft. Hersteller beherrschen die Komplexität in vielen Fällen nicht ausreichend und wenden etablierte Verfahren des Software Engineering nicht adäquat an.



Abhängig von der Klassifizierung existieren mehrere Möglichkeiten, ein Konformitätsbewertungsverfahren zu durchlaufen (Abb. 1).

Entscheidend für die Klassifizierung ist, für was der Hersteller das Produkt vorgesehen hat. Betriebssysteme, Entwicklungswerkzeuge oder Datenbanken sind keine Medizinprodukte, auch wenn sie für deren Entwicklung eingesetzt werden oder sogar deren integraler Bestandteil sind. Die Einschätzung einiger Experten, dass die elektronische Gesundheitskarte und die dazu notwendige Telematik-Infrastruktur die Kriterien erfüllen, wird kontrovers diskutiert [2].

Welche Folgen die Klassifizierung als Medizinprodukt für Hersteller, Betreiber und Anwender hat, zeigt ein Blick auf das hierarchisch aufgebaute europäische Rechtssystem. Zuoberst stehen die europäische sowie die nationalen Verfassungen (in Deutschland das Grundgesetz). Darunter finden sich auf europäischer Ebene die Richtlinien (Directives), die von den Mitgliedsländern in nationales Recht umgesetzt werden müssen. Während das Parlament (Bundestag, gegebenenfalls Bundesrat) Gesetze verabschiedet, können Regierung und Ministerien Verordnungen direkt erlassen.

Es gibt drei europäische Richtlinien zum Thema, nämlich die erwähnte 93/42 für allgemeine Medizinprodukte, 98/79 für In-vitro-Diagnostik (Laborgeräte) sowie 90/385 für aktive implantierbare medizinische Geräte. Das Medizinproduktegesetz (MPG) setzt alle drei in nationales Recht um. Es verlangt, dass Medizinprodukte ein Konformitätsbewertungsverfahren durchlaufen müssen. Hier wird festgestellt, dass der Hersteller über ein Qualitätsmanagementsystem (QMS) verfügt und ob das Produkt grundlegenden Anforderungen genügt. Letztere müssen die Sicherheit von Patienten und Anwendern bestmöglich gewährleisten. Die Anbieter weisen dies nach, indem sie „harmonisierte Normen“ erfüllen. Das sind solche, die das Amtsblatt der EU für die jeweilige Direktive nennt. Wohlgemerkt: Auch diese Normen sind nicht gesetzlich verpflichtend. Allerdings dürfte ohne sie der Nachweis schwer zu erbringen sein, dass man die Forderungen der Richtlinie und damit des MPG einhält.

Abgrenzung mit Konsequenzen

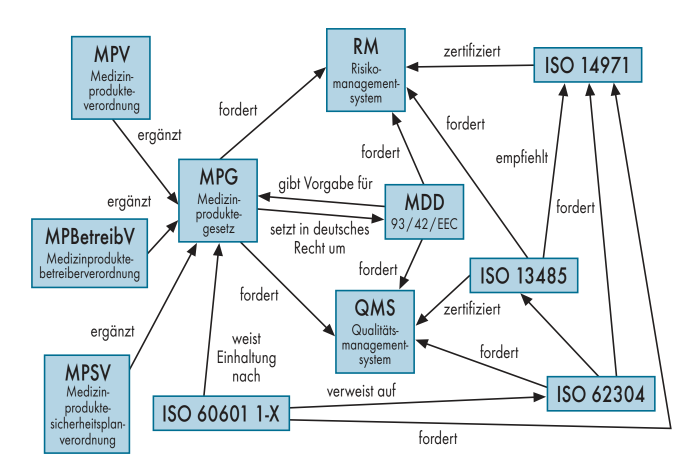
Zusätzliche Vorschriften ergänzen das MPG. Unter anderem regelt die Medizinprodukte-Betreiberverordnung, welche Personen das Produkt anwenden dürfen, wie sie zu schulen sind und wie Dokumentation und Wartung auszusehen haben. Ob eine Software als Medizinprodukt eingestuft wird oder nicht, wirkt sich also direkt auf Anwender und Betreiber aus. Über die Folgen, speziell für Krankenhäuser, gibt es zurzeit eine intensive Debatte.

Das MPG beschreibt mehrere Möglichkeiten, wie sich ein Konformitätsbewertungsverfahren durchlaufen lässt (Abbildung 1). Welche Optionen tatsächlich zur Auswahl stehen, hängt von der Klassifizierung des Produkts ab. Man unterscheidet die Klassen I, IIa, IIb und III, wobei höhere Klassen ein höheres Risiko bedeuten. Die Einordnung entscheidet sich beispielsweise anhand folgender Fragen: Gibt es Kontakt oder eine Integration mit dem menschlichem Körper (invasiv)? Wie lange dauert die invasive Prozedur und welcher Art ist sie? Handelt es sich um ein aktives Gerät (nutzt es beispielsweise elektrische Energie)? Wird es an lebenswichtigen Organen angewendet?

Software fällt unter die Definition „aktives Medizinprodukt“. Falls sie ein Medizingerät steuert oder beeinflusst, gehört sie in dieselbe Klasse. Bei Produkten der Klasse I (ohne Messfunktion) darf das Unternehmen die Konformität selbst erklären, ohne eine benannte Stelle einzuschalten. Für alle anderen Produkte gibt es prinzipiell zwei verschiedene Wege. Der erste wäre: Der Hersteller entwickelt das Produkt, um es anschließend zu prüfen beziehungsweise prüfen zu lassen. Die sogenannte Baumusterprüfung (Anhang III MPG) gehört zu diesem Verfahren. Im Anschluss muss er durch ein Qualitätsmanagementsystem nachweisen, dass er die Produkte entsprechend dem Baumuster produzieren kann. Die zweite Variante: Er verfügt über ein zertifiziertes vollständiges QMS, sowohl für die Entwicklung als auch für die Produktion. In diesem

Onlinequellen

Bundesamt für Arzneimittel und Medizinprodukte	www.bfarm.de
benannte Stellen	www.dimdi.de/static/de/mpg/adress/benannte-stellen/
harmonisierte Normen	ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html
Gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte	www.gematik.de
Software and Medical Devices, Hinweise zum Zulassungsverfahren	www.meddev.info/_documents/R2_2-4_rev5.pdf
Fachzeitschrift für Medizintechnik	www.mt-medizintechnik.de
TÜV Rheinland	www.tuv.com/de/medizinprodukte.html



Leicht zu durchschauen ist der Zusammenhang von Direktiven, Gesetzen, Normen und Verordnungen nicht (Abb. 2).

Fall darf der Anbieter die Konformität für sein Produkt ohne externe Prüfung ebenfalls selbst bestätigen.

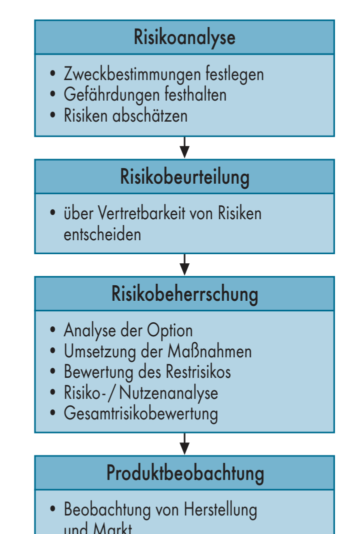
Den Nachweis über alle genannten Punkte führt er wie oben angedeutet über das Einhalten harmonisierter Normen (Abbildung 2). Es gibt Normen zu Qualitätsmanagementsystemen (ISO 13485), zum Risikomanagement (ISO 14971), zur Gebrauchstauglichkeit (IEC 60601-1-6) sowie demnächst eine zu Entwicklungsprozessen für medizinische Software (IEC 62304). Das Erfüllen dieser Vorgaben muss sich das Softwarehaus durch akkreditierten Stellen zertifizieren lassen, die damit indirekt das Produkt prüfen.

Software als Risikofaktor

Bisher Dargestelltes gilt für jedes Medizinprodukt. Software unterscheidet sich jedoch in einigen Punkten von klassischen Medizingeräten. Sie lässt sich als immaterielles Gut leicht kopieren und verteilen. Im Gegensatz zur Hardware leidet sie nicht an Verschleiß, allerdings altern Anwendungen indirekt, wenn Betriebssystem, Treiber und andere Programme sich ändern. Ebenfalls im Gegensatz zur Hardware sind Defekte Konstruktions- und fast nie Produktionsfehler. Software lässt sich nur sehr schwer vermessen, ein Grund dafür, dass sie in der Regel fehlerbehaftet ist. Ihre einfache Änderbarkeit führt zu einem ständigen Anpassungsdruck. Eine der Konsequenzen: Laut FDA werden 79 Prozent der Fehler erst nach der initialen Entwicklung eingeführt. Davon zeugen auch die Meldungen des BfArM.

Die benannten Stellen vertreten die Ansicht, dass der Einsatz von Software als Medizinprodukt eine solche Komplexität erreicht hat, dass sich systematische Fehler bei einem in der Praxis akzeptablen Prüfaufwand nicht mehr verlässlich erkennen lassen. Aus diesem Grund fordern sie zum einen, dass die Hersteller zusätzliche Prozesse (etwa Risiko- und Konfigurationsmanagement) etablieren und dokumentieren müssen. Zum anderen folgern sie, dass eine rein produktbezogene Bewertung ohne Einbeziehen des Designprozesses nicht ausreicht. Daher stufen sie einige Konformitätsbewertungsverfahren als für Software ungeeignet ein. Mit anderen Worten: Die Baumusterprüfung kommt für Software nicht infrage. Stattdessen ist ein Konformitätsbewertungsverfahren nach Anhang II (vollständiges Qualitätsmanagementsystem) vorzuziehen.

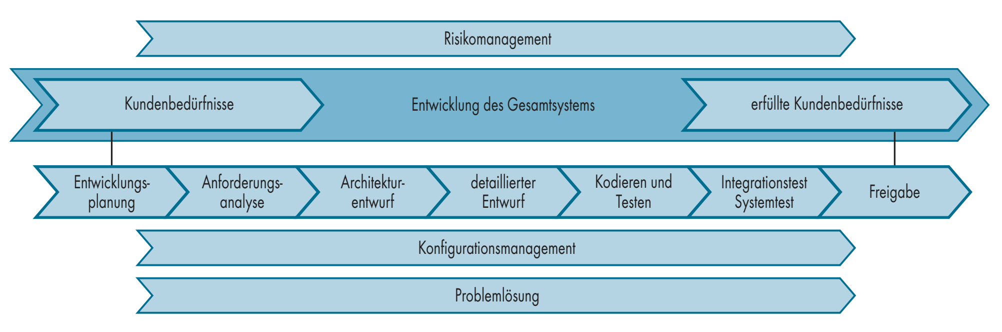
Die ISO 13485 zertifiziert Qualitätsmanagementsysteme. Sie gleicht der ISO 9001 weitgehend, enthält aber zusätzliche, für Medizinprodukte spezifische Forderungen. Wie die ISO 9001 verlangt sie Prozesse zur Produkterstellung, Verifikation und Validierung sowie produktspezifische Testaktivitäten und Akzeptanzkriterien (Abschnitt 7.1), Kunden- und Produktanforderungen sind zu dokumentieren (Abschnitt 7.2). Abschnitt 7.3 fordert Verfahren für Design und Entwicklung, Review, Verifikation und Validierung. Letztere soll sicherstellen, dass die Vorgaben für die Phasen Design und Entwicklung geprüft werden. Das Risikomanagement müssen die Hersteller in den Entwicklungsprozess integrieren.



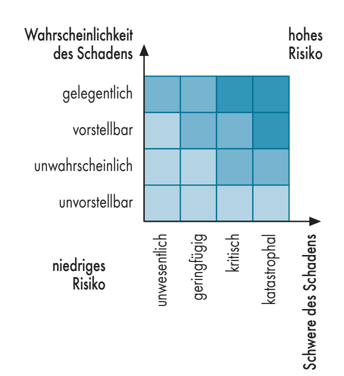
Die ISO 14971 verlangt ein prozessorientiertes Risikomanagement (Abb. 4).

Struktur für die Entwicklung

Explizit verlangt die IEC 60601-1-4, dass die Entwickler ihre Arbeit an einem Lebenszyklus- beziehungsweise Prozessmodell mit Meilensteinen ausrichten (IEC steht für „International Electrotechnical Commission“, die Normungsbehörde hat ihren Sitz in Genf). Für jeden Meilenstein sollen sie definieren, welche Tätigkeiten abgeschlossen sein müssen und wie diese zu verifizieren sind. Ein spezielles Lebenszyklusmodell wird nicht gefordert, allerdings zeigt die exemplarische Grafik ein V-Modell. Die Norm verlangt zusätzlich ein Risikomanagement nach ISO 14971 und verweist in ihrer dritten Ausgabe bereits auf die IEC 62304 für Softwareentwicklung. Ursprünglich sollte diese Norm regeln, wie Software für Medizingeräte zu entwickeln ist. Die Validierung des Gesamtsystems gehörte folglich nicht zu ihren Aufgaben. Dann erweiterte man ihre Anwendbarkeit auf Software als eigenständiges Medizinprodukt. Die IEC 60601-1-4 deckt allerdings weiterhin die Validierung ab.



Die IEC 62304 fordert Prozesse für Softwareentwicklung, Problemlösung, Risiko- sowie Konfigurationsmanagement (Abb. 3).



Die Qualitätspolitik legt nicht akzeptable (dunkelblau) und akzeptable Risiken (hellblau) sowie einen ALARP-Bereich (as low as reasonable possible, mittelblau) fest (Abb. 5).

Ob all die in Abbildung 3 dargestellten verschiedenen Phasen der Softwareentwicklung zu durchlaufen sind, hängt von der Risikoklasse ab. ISO 62304 definiert drei: Bei Klasse-A-Software können keine Verletzungen oder Gesundheitsschädigungen auftreten, bei Klasse B sind keine schweren Verletzungen möglich, und bei Klasse C kann sogar der Tod eintreten.

Die Wartung gleicht dem Entwicklungsprozess. Beim Risikomanagement verweist IEC 62304 verpflichtend auf ISO 14971. Auch verlangt Erstere ein QMS und empfiehlt eines gemäß ISO 13485. Wie IEC 60601-1-4 besteht die ISO 62304 nicht auf einem speziellen Prozessmodell, nennt aber ebenfalls exemplarisch das V-Modell. Laut ISO 14971 hat das Risikomanagement prozessorientiert zu erfolgen (Abbildung 4). Unter einem Risiko versteht diese Norm die Kombination aus der Wahrscheinlichkeit und dem Schweregrad eines Schadens (zum Beispiel Verletzung eines Patienten oder Anwenders). Eine hohe Wahrscheinlichkeit und ein großer Schaden ergeben folglich ein hohes Risiko. Alle identifizierten Risiken trägt man in eine spezielle Tabelle ein (Abbildung 5). Viele Risiken sind initial nicht akzeptabel. Gelingt es, sie auf ein akzeptables Niveau zu senken, dürfen die Anbieter das Produkt in den Verkehr bringen. Ob die eigenen Risikoeinschätzungen stimmen, müssen sie in einer nachgelagerten Phase beobachten.

Schwaches Risikobewusstsein

Bei der Vielzahl der beteiligten Normen entsteht leicht der Verdacht auf bürokratischen Overkill, was jedoch nur zum Teil zutrifft. Denn: Liest man die Meldungen des BfArM, erhält man nicht den Eindruck, als würden die Beteiligten die Komplexität medizinischer Software ausreichend beherrschen. Und wer die Anforderungen IEC 62304 studiert, findet im Wesentlichen Forderungen, die für eine professionelle Softwareentwicklung (nicht nur im medizinischen Umfeld) selbstverständlich sein sollten. Wünschenswert wäre, dass die Betreiber ein höheres Bewusstsein für die Risiken entwickeln, die das Zusammenschalten von IT und Medizingeräten auslöst. Man ahnt es schon, eine neue Norm hierfür (IEC 80001) entsteht gerade. (jd)

DR. CHRISTIAN JOHNER

ist Professor an der Hochschule Konstanz und leitet in Freiburg das Institut für IT im Gesundheitswesen. Als Berater unterstützt er Firmen bei der Entwicklung und Zulassung medizinischer Software.

Literatur

[1] Armin Gärtner; Medizintechnik und Informationstechnologie; Bde. 1 – 4, TÜV Media, 2005–2007

[2] Jürgen Stettin, medizintechnik, 6/2007, S. 202






Object-Based Storage Devices

Gekapselt

Oliver Tennert

Als ehernes Gesetz galt bislang, dass ein Massenspeicher für wahlfreien Zugriff ein Blockgerät sein muss. Object-Based Storage Devices speichern jedoch keine Blöcke, sondern Datenobjekte, bieten eine starke Zugriffskontrolle und stellen für Storage im High Performance Computing das zukunftweisende Konzept dar.

Etwa 1983 kamen die ersten SCSI-Festplatten in den Handel – drei Jahre, bevor das American National Standards Institute (ANSI) den offiziellen SCSI-Standard verabschiedete. Seitdem hat sich das grundlegende SCSI-Protokoll (mittlerweile in Version 3) nicht wesentlich geändert. Es sind neue physikalische Schnittstellen beziehungsweise Transportschichten wie Fibre Channel, iSCSI oder SAS hinzugekommen. Jedoch war eine SCSI-Platte – ebenso wie später IDE- und SATA-Platten – immer ein Blockgerät, von dem man linear adressierte Blöcke fester Größe lesen und schreiben kann. Object-Based Storage Devices (OSD) hingegen arbeiten auf der darüberliegenden (Datei-)Ebene.

Begonnen hat die Geschichte des objektorientierten Speichers 1994 an der Carnegie Mellon University (CMU) im Rahmen des durch die US-Regierung geförderten Projekts Network Attached Secure Disk (NASD, siehe Kasten „Onlinequellen“). Garth Gibson, bekannt durch sein „RAID-Papier“, und andere Mitarbeiter erarbeiteten ein Konzept, das den Overhead eines Fileservers reduzieren sollte. Dazu verlagerten sie das Space-Management – die Blockallozierung – in das Storage-Gerät. Die häufigen Lese- und Schreiboperationen der Nutzdaten gehen von den Clients direkt an das Device, das die gewünschten Daten in Form von Objekten variabler Länge statt in Blöcken fester Länge zurückschickt. Außerdem führt das Gerät die Zugriffskontrolle durch, während die Authentifizierung Aufgabe des Fileservers bleibt.

Im Laufe der Jahre erfuhr das NASD-Projekt große Unterstützung durch die Industrie. Kommerzielle Produkte wie das ActiveScale PanFS der später von Garth Gibson mitgegründeten Firma Panasas und das konzeptionell verwandte Dateisystem Lustre von Peter Braam haben ihre Ursprünge ebenfalls an der CMU. Standardisierungsbestrebungen, zunächst vorangetrieben durch das National Storage Industry Consortium (NSIC), später durch die OSD Technical Working Group der Storage Networking Industry Association (SNIA), mündeten 2004 in einen Draft Standard für Object-Based Storage Devices des für das SCSI-Interface zuständigen ANSI-Kommitees T10. Im September 2004 ratifiziert, wurde dieser zum offiziellen Standard ANSI INCITS 400-2004. Die aktuellen Anstrengungen gehen in die Erweiterung OSD-2, die seit Juli 2008 in der aktuellen Revision 4 vorliegt. Neben Erweiterungen wie Snapshots, Multi-Objekt-Operationen und Collections spezifiziert OSD-2 vor allem eine verbesserte Fehlerbehandlung.

Alles ist ein Objekt

Hinter einem Object-Based Storage Device verbergen sich letztendlich auch handelsübliche Festplatten mit sich drehenden Scheiben und einer Reihe von Sektoren, die fortlaufend nummeriert sind. Der Unterschied besteht darin, dass man auf die Sektoren nicht direkt zugreifen kann. Vielmehr stellt die objektorientierte Schnittstelle alle Daten als logische Entitäten dar. Um das Speichermanagement – welche Sektoren welche Daten enthalten – kümmert sich das OSD selbst (siehe Abbildung 1).

Es setzt so den Trend fort, immer mehr Funktionen auszulagern und dadurch den Rechner zu entlasten. In den Kindertagen der Festplatte etwa steuerte noch das Betriebssystem des Computers die Bewegungen der Schreib-/Leseköpfe.

Jedes Objekt ist als fundamentale Speichereinheit eines OSDs in sich vollständig. Es besteht aus einer 64 Bit langen Object ID (OID), weiteren Attributen wie Zeitstempel, Besitzerinformationen, Größe oder dem – von außen nicht sichtbaren – physikalischen Speicherort innerhalb des OSD sowie den Nutzdaten. Alle Objekte innerhalb eines OSD bilden einen flachen Namensraum – die Abbildung eines Verzeichnisbaums muss das Host-Betriebssystem durch Referenzierung über Zeiger realisieren.

Der aktuelle Draft des OSD-Standards definiert vier Arten von Objekten (siehe Abbildung 2). Neben dem sogenannten Wurzel- oder Root-Objekt – hinter dem sich nichts anderes als das OSD selbst verbirgt – sind die wichtigsten die sogenannten Benutzerobjekte (user objects). Sie stellen die eigentlichen „Da-

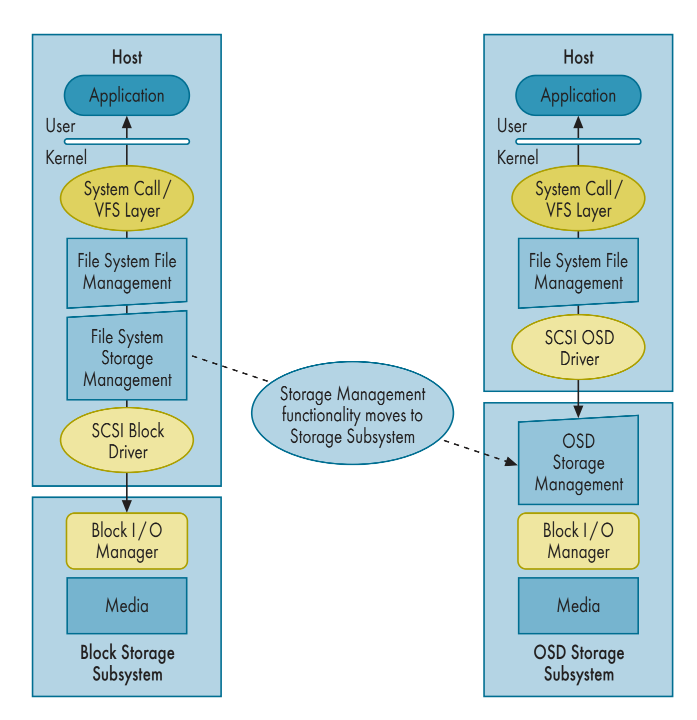
teien“ dar und lassen sich von einer Applikation beziehungsweise dem Betriebssystem des Host über SCSI-Kommandos erzeugen. Sammelobjekte (collection objects) enthalten Benutzerobjekte, die nach gewissen Kriterien zusammengefasst wurden; Partitionen (partition objects) sind Container für Benutzer- oder Sammelobjekte und besitzen gemeinsame Sicherheits- und Space-Management-Charakteristika wie Quotas oder Schlüssel.

Als „Name“ respektive „Adresse“ eines Objekts dient die Kombination aus einer Partition ID (32 Bit) und einer gleich langen User Object ID. Hat Letztere den Wert *0*, bezeichnet die Adresse eine Partition; Partition *0* kennzeichnet das Root-Objekt. Insgesamt erlaubt das Adressierungsschema gut vier Milliarden Partitionen, die jeweils ebenso viele Benutzer- oder Sammelobjekte enthalten können.

Attribute für alle

Jedes Objekt kann bis zu 2^{32} Attributseiten mit jeweils maximal 2^{32} Attributen besitzen. Nur eine kleiner Teil des Namensraums ist vordefiniert, etwa für Zeitstempel oder Benutzernamen. Der Rest steht dem Host zur freien Verfügung, etwa für erweiterte Dateiattribute.

Beim Zugriff auf ein Objekt kann jede Schicht der Speicherimplementierung Attribute interpretieren und sich darauf basierend unterschiedlich verhalten, angefangen vom OSD selbst über Kerneltreiber bis hin zu höheren Betriebssystemschichten. Nicht interpretierte („opake“) Attribute werden unverändert an die nächste Schicht weitergereicht. Auf diese Weise kann man etwa auf der Betriebssystemebene einige Objekte als hochverfügbar, andere als temporär

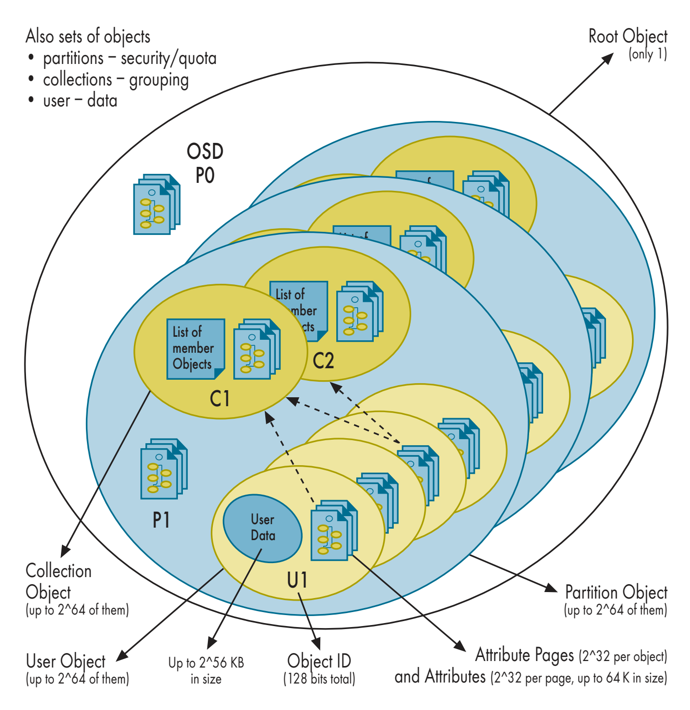


Entlastung: Bei objektbasierten Speichern muss sich der Rechner nicht um die Zuteilung von Datenblöcken kümmern (Abb. 1).

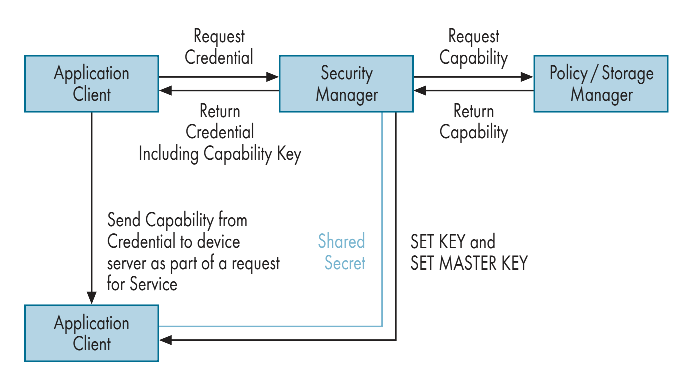
kennzeichnen. Da Attribute objektgebunden sind, bleiben sie auch beim Kopieren von Objekten von einem auf ein anderes OSD erhalten.

Der OSD-Standard definiert ein auf Capabilities („Fähigkeiten“) basierendes Zugriffsprotokoll mit starker kryptografischer Sicherheit,





Aktenordner: Container- und Sammelobjekte enthalten Objekte mit gleichen oder ähnlichen Eigenschaften (Abb. 2).



Türsteher: Clients müssen alle Zugriffe erst vom Security Manager beglaubigen lassen (Abb. 3).

Onlinequellen

Network Attached Secure Disks Publications
www.pdl.cmu.edu/NASD/

SCSI Object-Based Storage Device Commands (OSD) Working Draft
www.t10.org/ftp/t10/drafts/osd/osd-r10.pdf

SCSI Object-Based Storage Device Commands-2 (OSD-2) Working Draft
www.t10.org/ftp/t10/drafts/osd2/osd2r04.pdf

Lustre File System
www.sun.com/software/products/lustre/

Lustre Wiki
www.lustre.org

IBM Object Storage Device Simulator for Linux
www.alphaworks.ibm.com/tech/osdsim

IBM Haifa Labs – Object Store
www.haifa.ibm.com/projects/storage/objectstore/objectstone.html

IBM OSD Initiator
sourceforge.net/projects/osd-initiator

Object Storage Device (OSD) support for Solaris
opensolaris.org/os/project/osd/

das die Integrität eines SCSI-Request und den legitimen Gebrauch durch den Client sicherstellt. Jedes Kommando ist mit einem Message Authentication Code (HMAC-SHA1, 160 Bit) versehen, der das spezifische Objekt und die Liste von Operationen identifiziert, die auf das Objekt wirken können.

Abbildung 3 illustriert den Zugriffsprozess. Will ein Client auf ein Objekt zugreifen, muss er dafür vom Security Manager die Erlaubnis erbitten. Der fragt den Policy Manager, ob der Client die gewünschte Aktion ausführen darf. Ist die Operation erlaubt, generiert der Security Manager ein Credential, das die vom Policy Manager gelieferte Capability und einen Integritätsprüfwert (Capability Key) enthält, und übergibt es an den Client. Den Capability Key generiert er mithilfe einer Pseudozufallsfunktion aus der Capability und einem zuvor mit dem OSD vereinbarten geheimen Schlüssel (Working Key).

Der Client reicht die Capability mit seinem Request zur Verifikation ans OSD weiter. Hält sie der Überprüfung stand, führt das OSD die Operation aus. Zur Abkürzung des Verfahrens kann der Client ein Credential für mehrere Operationen erfragen – etwa lesen, schreiben und löschen – und vorsorglich in einem lokalen Cache aufbewahren. Bei Bedarf kann er es auch an einen anderen Client weiterreichen. Der Security Manager kann Credentials mit begrenzter Gültigkeitsdauer ausstellen oder noch gültige widerrufen.

Aus Sicherheitsgründen sollte der Security Manager den Working Key regelmäßig wechseln. Allerdings verlieren dann die daraus erzeugten Capability Keys ihre Gültigkeit. Alle Clients müssen neue Credentials beantragen, und das OSD muss sie erneut verifizieren. Daher kommt es bei einem Schlüsselwechsel zu Performance-Einbußen. Als Gegenmaßnahme kann ein OSD bis zu 16 gültige Working Keys vorhalten. Kommt ein neuer hinzu, wirft es den ältesten weg.

Objektorientierter Speicher ist heute schon weit verbreitet, ohne dass es auffällt: Lustre und ActiveScale PanFS von Panasas sind prominente Software-Implementierungen eines objektorientierten Speicherzugriffsprotokolls für HPC-Storage, wobei PanFS weitgehend standardkonform ist. Lustre hingegen hebt sich deutlich vom OSD-Standard ab. Parallel NFS, Teil von NFS 4.1, unterstützt OSD-konformen Zugriff auf parallelen Speicher.

EMCs Archivsystem Centera kann man als eine eingeschränkte Form von objektorientiertem Speicher betrachten, die nur einen Teil des T10-Standards unterstützt – obendrein auf proprietäre Weise. Andererseits zielt die Centera vorrangig auf Compliance ab und bietet Content Addressable Storage (CAS), wobei die Objekte – die im Wesentlichen direkt über ihre Hash-Werte adressiert werden – unveränderlich sein sollen (Fixed Content Storage).

IBM war in der Vergangenheit in Sachen OSD-Unterstützung für Linux recht aktiv: Die Haifa Labs arbeiten im Rahmen des Projekts „Object Store“ an „ObjectStone“, dem Prototyp eines objektorientierten Storage-Controllers. Aktuelle Versionen von ObjectStone beinhalten ein OSD-Target in Form eines Linux-Kerneltreibers. Daneben bietet das Unternehmen einen OSD-Simulator für Testzwecke und einen OSD-SCSI-Initiator als Open Source an. Der aktuelle Code stammt allerdings aus dem Jahr 2005, und bis zur offiziellen Verabschiedung von OSD-2 dürfte sich daran nicht viel ändern.

(mr)

DR. OLIVER TENNERT

ist Head of Technology bei der Tübinger transtec AG.




Sicherheitslücken durch Seitenkanalattacken

Torschlusspanik

Thomas Eisenbarth, Timo Kasper, Christof Paar



Dass auch Kleinstcomputer sicherheitskritische Systeme sind, vergisst man leicht. Doch ein erfolgreicher Angriff auf die Keeloq-Funktüröffner scheint die Hersteller aus ihrem Dornröschenschlaf gerissen zu haben. Die Forscher, die das System im März dieses Jahres geknackt haben, berichten über die technischen Details.

Funktüröffner für Garagen-, Haus- und Autotüren sind weithin beliebt – aber leider längst nicht so sicher, wie Anwender glauben und Herstelleraussagen versprechen. Denn die dort eingesetzte Implementierung des Keeloq-Algorithmus kann mit relativ preiswertem Equipment ausgehebelt werden. Um zu verstehen, wie das genau passiert und was man dagegen tun könnte, ist ein näherer Blick auf die sicherheitstechnischen Funktionen dieser Systeme nötig.

Die erste Generation der Funktüröffner war mit Fixcode-Systemen ausgestattet, die bei jedem Druck auf den Knopf des Handsenders dieselbe Folge von Nullen und Einsen an den Empfänger sendeten. Schon nach kurzer Zeit hatten Kriminelle herausgefunden, dass man die Codes in einem Umkreis von 100 m abfangen und später wieder abspielen kann – die Zahl von Diebstählen stieg an.

Neues Spiel – neuer Code

Als Reaktion auf diese Replay-Attacken entstanden Wechselcode-Systeme, die bei jedem Knopfdruck einen neuen Code generierten. Ausgangsbasis für die Erzeugung dieser Hopping Codes ist ein Zähler, den der Sender bei jeder Betätigung um eins erhöht und verschlüsselt an den Empfänger überträgt. Der entschlüsselt den empfangenen Code und vergleicht den erhaltenen Zählerstand mit dem bei ihm gespeicherten. Ist der empfangene Wert größer, wird die Funktion ausgeführt und der neue Zählerstand vom Empfänger übernommen. Kommt ein veralteter, zu niedriger Zählerstand an, wird er ignoriert, was Replay-Attacken unmöglich macht.

Als Chiffre zur Erzeugung der Geheimtexte dient im Fall der hier behandelten Funktüröffner mit Wechselcode der Keeloq-Algorithmus, eine 32-Bit-Blockchiffre mit 64-Bit-Schlüssel. Der Klartext wird in Pakete von 32 Bit Länge aufgeteilt, die einzeln verschlüsselt und zu einem Geheimtext zusammengefügt werden. Um den geheimen Schlüssel zu erraten, müsste man alle möglichen Kombinationen ausprobieren – die Anzahl der nötigen Versuche entspricht einer Zahl mit 19 Nullen und ist somit für einen Brute-Force-Angriff zu groß.

iX-TRACT

- Eingebettete Systeme verzichten aus Kostengründen oft auf starke Sicherheitsmechanismen.
- Das für Auto-, Garagen- und Haustüren breit eingesetzte Keeloq-Verfahren ist durch eine Seitenkanalattacke geknackt worden und nicht mehr sicher.
- Seitenkanalattacken sind ein generelles Problem von Security-Implementierungen, die zwar kryptografisch sicher sind, aber zu wenig Wert auf das Unkenntlichmachen von Abstrahlung und Stromverbrauch legen.

In riesigen Stückzahlen gefertigte ASICs für die Erzeugung von Hopping Codes mit der Keeloq-Chiffre [6] und die Einfachheit des Keeloq-Algorithmus ermöglichen äußerst günstige Preise bei der Herstellung. Daher verbreitete sich die von der Firma Microchip Technology Inc. lizenzierte Keeloq-Chiffre seit ihrer Erfindung in den 80er-Jahren über OEMs weltweit, zum Beispiel in Funktüröffnern für Garagen.

2007 beschäftigte sich erstmalig der Kryptologe Andrey Bogdanov mit der Kryptanalyse der Keeloq-Chiffre [1]. Seine Attacke wurde kurz darauf von einer belgisch-israelischen Forschergruppe verbessert [11],

Wie Keeloq funktioniert

Die Keeloq-Chiffre besteht im Wesentlichen aus einer nichtlinearen Funktion (NLF) und zwei Schieberegistern – einem Zustandsregister mit einer Länge von 32 Bit und einem Schlüsselregister mit 64 Bit. Das Zustandsregister wird zunächst mit dem Klartext geladen. Dann erfolgt in jedem Takt eine Verschiebung der Bits in den Registern um eine Position nach links sowie die Verknüpfung einiger Bits des Zustandsregisters mit einem Schlüsselbit unter Zuhilfenahme der NLF- und XOR- Funktionen. Nach 528 Taktzyklen ist die Verwürfelung vollzogen und das Zustandsregister enthält den Geheimtext. Die Chiffre erzeugt also auch bei sehr kleinen Änderungen des Klartextes (zum Beispiel ein gekipptes Bit) völlig unterschiedliche, neue Geheimtexte, die theoretisch ein Finden der zugehörigen Klartexte ohne Kenntnis des Schlüssels unmöglich machen.

Für die Erzeugung der Hopping Codes geht nun als Klartext der aktuelle Zählerstand des Handsenders, die gewählte Funktion (für Handsender mit mehreren Knöpfen) und ein sogenannter „Discrimination Value“ ein. Letzterer ist für ein Funktüröffnersystem konstant und ermöglicht dem Empfänger durch Vergleich mit dem eigenen Discrimination Value nach dem Entschlüsseln zu entscheiden, ob die empfangenen Daten gültig sind oder ob beispielsweise zufällig generierte Nachrichten verschickt wurden. Dem verschlüsselten Teil der Nachricht wird im Klartext die eindeutige Seriennummer des Handsenders und erneut die gewählte Funktion vorangestellt.

sodass, ausgehend von etwa 65 000 bekannten Paaren von Klar- und Geheimtexten, 50 Dual-Core-Computer in der Lage sind, binnen einer Woche den geheimen Schlüssel zu finden. Somit ist Keeloq mathematisch gebrochen, also kryptografisch unbrauchbar. Im Kontext von Funktüröffnern sind diese Attacken jedoch nicht umsetzbar, weil der Klartext zur Erzeugung der Hopping Codes für den Angreifer unzugänglich im Chip des Handsenders verbleibt.

Angriff ganz ohne Klartext

Doch die von den Autoren dieses Artikels durchgeführten Angriffe benötigen den Klartext **nicht** und sind obendrein in erheblich kürzerer Zeit und mit erheblich geringerem Aufwand durchführbar.

Ein Blick auf die Implementierung verdeutlicht die Schwächen: Als geheimer Schlüssel für die Erzeugung des Geheimtexts wird ein pro Sender eindeutiger Senderschlüssel verwendet. Der Handsender erhält diesen Schlüssel schon während seiner Produktion. Doch wie erfährt ihn der Empfänger? Die Antwort lautet: Schlüsselableitung mittels eines eindeutigen Herstellerschlüssels, den jeder OEM erhält. Mit dessen Kenntnis lässt sich, zum Beispiel aus der empfangenen Seriennummer, der individuelle Handsenderschlüssel berechnen.

Zur Ableitung der 64 Bit des Senderschlüssels müssen zwei Keeloq-Entschlüsselungen durchgeführt werden. Die Funktionen zur Anpassung der Seriennummer an die Blockgröße von 32 Bit sind typischerweise sehr einfach gehalten, zum Beispiel Auffüllen (sog. Padding) mit Nullen. Neben der Schlüsselableitung aus der (im Klartext jeder Nachricht enthaltenen) Seriennummer erlauben manche Modelle von Keeloq-Funktüröffnern die Schlüsselableitung aus einem zufällig für jeden Handsender vergebenen „Seed“ mit Bitlängen von 32, 48 oder 60 Bit, den der Sender zum Beispiel durch Druck auf eine Sondertaste während des Anlernvorgangs sendet.

Der Herstellerschlüssel wird in jedem Empfänger in einem geschützten, nicht auslesbaren Speicher vorgehalten. Vor der ersten Benutzung eines neuen Handsenders muss also der Empfänger dessen Senderschlüssel in einem Anlernvorgang mittels des Herstellerschlüssels ableiten. Nach diesem pro Schlüssel einmaligen Lernvorgang kennt der Empfänger den zur Seriennummer gehörenden Senderschlüssel und kann auf die von diesem Handsender erzeugten Hopping Codes reagieren.

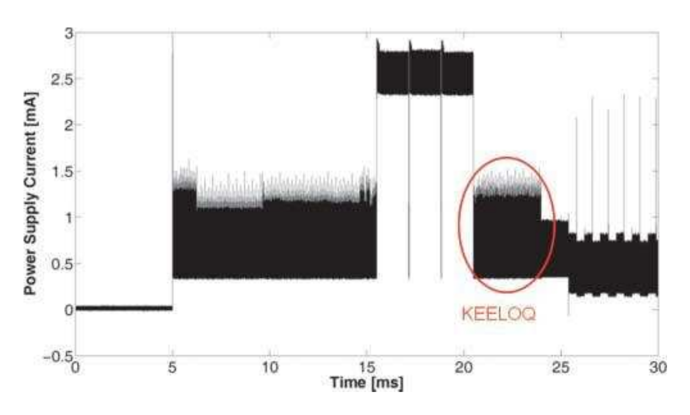
Königsweg Seitenkanalanalyse

Um die Methode der Autoren zum Aushebeln des Keeloq-Verfahrens zu verstehen, muss man sich vergegenwärtigen, dass elektronische Geräte während des Betriebs elektromagnetische Strahlung aussenden. Bei Mikroprozessoren und anderen ICs ist die elektromagnetische Emission zu einem gewissen Grad datenabhängig. Bei der sogenannten Seitenkanalanalyse nutzt man diese datenabhängige Strahlung, um an in der Implementierung versteckte Informationen zu gelangen, etwa geheime Schlüssel.

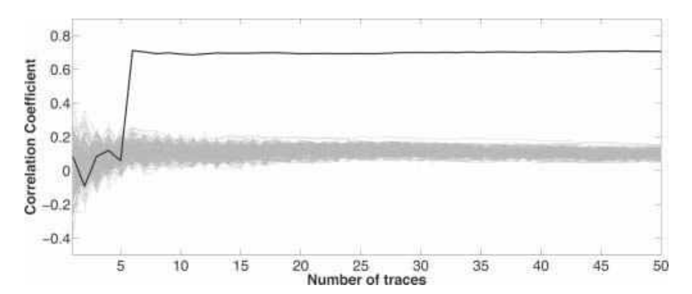
Verräterische Leistungsaufnahme

Seitenkanalanalyse kann so Implementierungen von kryptografischen Verfahren, die als mathematisch sicher gelten, brechen. Zur Durchführung eines Angriffs benötigt der Angreifer jedoch physischen Zugriff auf die Implementierung, um die Seitenkanalinformationen während der Verschlüsselung messen zu können. Klassischerweise wird neben der elektromagnetischen Abstrahlung auch der ebenfalls datenabhängige Stromverbrauch eines ICs zur Gewinnung von Informationen über den Seitenkanal genutzt.

Eine spezielle Art von Seitenkanalangriffen ist die Ende der 90er-Jahre entwickelte Differential Power Analysis (DPA, [8]) die bis heute



Eine exemplarische Messkurve des Senders mit klar abgrenzbarem Chiffrierteil (Abb. 1)



Die Korrelation für den richtigen Schlüssel (schwarz) und die falschen Schlüsselhypothesen (grau), aufgetragen über der Anzahl der benutzten Messungen – nach 10 Messungen ist der Fall klar (Abb. 2)

als eine der stärksten Seitenkanalattacken gilt. Dabei werden die Informationen mehrerer Verschlüsselungsvorgänge kombiniert, mit der Anzahl der aufgenommenen Messkurven steigt die Wahrscheinlichkeit für das Finden des korrekten Schlüssels. Eine DPA läuft für gewöhnlich in mehreren Schritten ab:

1. Analyse des anzugreifenden Verfahrens, das mit bekannten Daten nachvollziehbar sein muss, und Entwicklung eines Modells der Implementierung, das Stromverbrauch und Abstrahlung abhängig von Schlüssel, Klar- und Geheimtext vorhersagen kann.
2. Aufzeichnen der Seitenkanalinformationen und der Verschlüsselungsinformation während der Chiffrierung. Bei Leistungsmessungen wird die Stromaufnahme des Testchips durch einen mit dem Messobjekt in Reihe geschalteten Widerstand gemessen. Messungen des elektromagnetischen Feldes lassen sich mit einer direkt über dem Schaltkreis positionierten Nahfeldsonde durchführen.
3. Aufbereitung der Daten – Bereinigung von Rauschen, genaue zeitliche Zuordnung zu den einzelnen Schritten der Verschlüsselung.
4. Analyse der so gewonnenen Daten. Der gemessene Stromverbrauch wird mit einem vorhergesagten, schlüsselabhängigen Stromverbrauch korreliert. Zur Vorhersage dient das Modell aus dem ersten Schritt. Für den richtigen Schlüsselkandidaten ist die Korrelation am höchsten. Sind genügend Messungen vorhanden, lässt sich der richtige Schlüssel leicht von den falschen unterscheiden.

DPA kann sowohl gegen Hardware- als auch gegen Softwareimplementierungen, zum Beispiel auf Mikrocontrollern, eingesetzt werden, man muss nur jeweils das Stromverbrauchsmodell anpassen. Bei Mikrocontrollern korreliert der datenabhängige Stromverbrauch oft mit dem Hamminggewicht (also der Anzahl der Einsen im Wort) des verarbeiteten Registers. Details und weitere Verfahren sind in der Fachliteratur beschrieben [10].

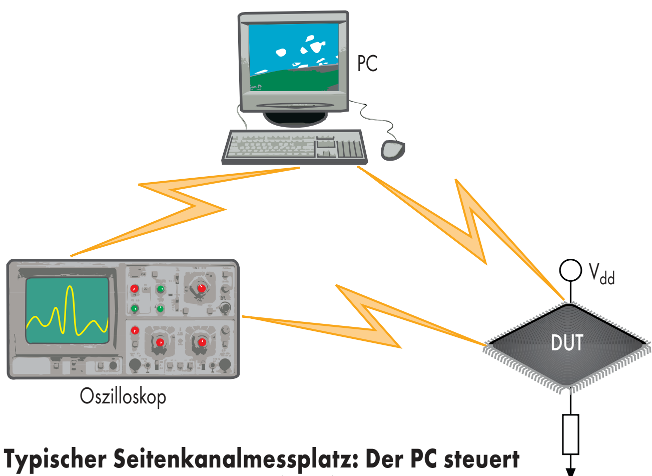
Im Falle von Keeloq ist die Verschlüsselungsroutine des Senders als ASIC realisiert, die Funktionen des Empfängers sind in Software, zum Beispiel auf einem Mikrocontroller, umgesetzt. Da Keeloq eine simple Chiffre ist, entspricht das hypothetische Stromverbrauchsmodell dem tatsächlichen Stromverbrauch sehr genau (Abb. 1). Hierdurch konnte eine mächtige Attacke entwickelt werden: Manchmal braucht es nur sechs Messkurven, aber immer reichen 30, um den Schlüssel eines Handsenders zurückzugewinnen.

Die Analyse des Empfängers gestaltete sich schwieriger. In den Messkurven ließ sich kein stabiler Triggerpunkt für das Oszilloskop identifizieren, weshalb sie trotz Nachbearbeitung noch relativ stark verrauscht waren. Für die Extraktion eines Schlüssels wurden darum rund 1000 Messungen benötigt.

Equipment für 1000 Euro reicht

Als Voraussetzungen benötigt der Angreifer einen Messaufbau, bestehend aus einem handelsüblichen PC und einem digitalen Speicheroszilloskop. Oszilloskope mit ausreichender Bandbreite und Speichertiefe sind für unter 1000 Euro erhältlich (s. Abb. 2). Zudem ist ein gewisses Vorwissen notwendig, etwa auf dem Level eines FH-Studiums Elektrotechnik oder Informationstechnik.

Was heißt das nun in der Praxis? Zum Klonen eines Senders benötigt der Angreifer Zugriff darauf, und er muss in der Lage sein, den beschriebenen Angriff durchzuführen. Er drückt den Knopf des Senders circa 30-mal und misst gleichzeitig die Abstrahlung oder die Leistungsaufnahme des Chips. Mit der DPA gelangt er so an



Typischer Seitenkanalmessplatz: Der PC steuert Oszilloskop und Testchip (DUT), das Oszilloskop misst die Leistungsaufnahme des Testchips über die Zeit; diese Kurve kann der PC analysieren (Abb. 3).

den geheimen Senderschlüssel. Damit kann er die Nachrichten des Senders entschlüsseln, den Zählerwert auslesen und eigene Nachrichten mit der gleichen Seriennummer und gültigen Zählerwerten generieren. Er hat also den Handsender geklont und kann sich Zugang zu dem geschützten System verschaffen.

Dieses Szenario trifft auf Fälle zu, in denen der Angreifer für zumindest wenige Minuten Zugang zum Handsender hat; beispielsweise ein Leihwagen, dessen Sender der Angreifer kopiert, um sich danach beliebig oft Zugang zu diesem Fahrzeug zu verschaffen. Da er für jedes Zielobjekt eine neue Seitenkanalanalyse durchführen muss, ist der durch diesen Angriff verursachte Schaden begrenzt. Der erforderliche Aufwand ist nur bei hochwertigen Zielen sinnvoll.

Ungleich folgenschwerer ist die Seitenkanalanalyse des Empfängers. Hier wird Keeloq nicht nur zur Entschlüsselung der Nachricht, sondern auch zur Ableitung des Senderschlüssels während der Lernphase verwendet. Analysiert man den Empfänger also während dieser Lernphase, so kann der Herstellerschlüssel extrahiert werden. Der Angreifer benötigt dazu einen Empfänger des entsprechenden Herstellers. Viele Funktüröffner, zum Beispiel Garagentoröffner oder Gebäudesicherungen, sind als Komplettsystem im Baumarkt erhältlich.

Nachbauten durch Schlüsselklau

Wer im Besitz des Herstellerschlüssels ist, kann für beliebige Seriennummern gültige Senderschlüssel generieren und folglich kompatible Sender und Empfänger produzieren. Bisher war dies dem Hersteller vorbehalten, der oft gut an dem Geschäft mit den kompatiblen Sendern verdient. Dieses Monopol ist durch das Bekanntwerden des Herstellerschlüssels gebrochen und der Markt für Billigprodukte offen. Für deren Hersteller könnte sich also der Aufwand, die oben beschriebene DPA durchzuführen, durchaus lohnen.

Der Herstellerschlüssel allein ermöglicht es aber noch nicht, jedes beliebige System des Herstellers zu öffnen, da die Empfänger nur auf bereits angelernte Seriennummern reagieren. Doch ist ein Angreifer in der Lage, Nachrichten eines angelernten Originalsenders aufzuzeichnen, kann er dessen Senderschlüssel bestimmen. Typischerweise ist der Senderschlüssel eine Funktion der im Klartext übertragenen Seriennummer und des Herstellerschlüssels. Mit dem durch Ausführen der Schlüsselableitung selbst berechneten Senderschlüssel kann der Angreifer nun die abgefangene Nachricht entschlüsseln, den Zählerstand ermitteln und eine neue gültige Nachricht generieren. Der Empfänger ist nicht in der Lage, den empfangenen Code von einem gültigen, vom Original-Sender erzeugten Hopping Code zu unterscheiden – im Handumdrehen schwingt das Garagentor auf. Der Angreifer benötigt dazu nur einen Empfänger zum Mitschneiden der Nachrichten, einen PC zur Bestimmung des Senderschlüssels in Echtzeit und einen Sender, um gültige Nachrichten zu senden. Abgesehen vom PC sind das Bauteile im Wert von circa 30 Euro.

Ist der Herstellerschlüssel erst bekannt, kann jeder Elektronikbastler den Lauschangriff durchführen. Wichtig ist, dass der Herstellerschlüssel zum Brechen aller Keeloq-Produkte dieses Anbieters nur ein einziges Mal extrahiert werden muss. Diesen Arbeitsschritt können erfahrene DPA-Spezialisten übernehmen, einmal extrahierte Schlüssel lassen sich über das Internet verbreiten.

Stark reduzierte Sicherheit

Auch ein Gerät, das Nachrichten mitschneidet, automatisch entschlüsselt und auf Knopfdruck Codes zum unbefugten Öffnen einer Tür sendet, könnte von Kriminellen, die im Besitz des Herstellerschlüssels sind, entworfen und vertrieben werden. Solch ein Gerät wäre von jedermann zu bedienen – ein Horrorszenario für viele Besitzer von Keeloq-Zugangssystemen. Die Sicherheit eines mit Keeloq gesicherten Systems ist infolge der oben vorgestellten Seitenkanalangriffe etwa auf die eines Fixcode-Systems reduziert. Der betriebene kryptografische Aufwand zur Erzeugung von Wechselcodes verpufft wirkungslos.

Den Angriff erschweren kann die Verwendung eines Seeds während der Schlüsselableitung. Während ein 32-Bit-Seed von einem einfachen PC in relativ kurzer Zeit erraten werden kann, ist der Lauschangriff für einen 60-Bit-Seed selbst mit spezieller kryptanalytischer Hardware wie der COPACOBANA [5] nur unter großem Zeitaufwand durchführbar. Leider wird diese Sicherheitsoption in der Praxis nur sehr selten genutzt, da sie den Anlernvorgang komplizierter macht. Außerdem waren Geräte, die nur kurze Seed-Längen zulassen, billiger und sind damit weiter verbreitet.

Der Lauschangriff kann noch weiter ausgebaut werden. Ein herkömmlicher Sender erhöht den Wert des Zählers mit jedem Druck auf den Knopf um eins. Ist der Angreifer in der Lage, gültige Nachrichten zu senden, kennt er auch den aktuellen Zählerstand. Im Gegensatz zum legitimen Nutzer kann er Nachrichten mit einem beliebigen Zählerstand generieren und den Zählerstand um einige Tausend erhöhen. Hiermit übernimmt er das komplette System. Der legitime Nutzer müsste mehrere Tausend Mal den Knopf seines Senders drücken, um wieder einen akzeptierten Zählerwert zu erreichen. Nur der Angreifer hat jetzt noch Zugang.

Fazit

Ausschlaggebend für den Erfolg der Angriffe auf Keeloq-Funktüröffner sind nicht die kryptografischen Eigenschaften der Keeloq-Chiffre, sondern die Mächtigkeit der Seitenkanalanalyse. Durch Messen des Stromverbrauchs können in wenigen Minuten kommerzielle Umsetzungen mathematisch sicherer Verschlüsselungen gebrochen werden. Dies gilt für jegliche ungeschützte Implementierung von Kryptografie: Selbst der AES (Advanced Encryption Standard), den die amerikanische NSA (National Security Agency) für Top-Secret-Nachrichten nutzt, widersteht DPA-Attacken nicht [10].

Sichere Umsetzungen von Verschlüsselung sind möglich, aber nicht umsonst zu haben. So finden sich bei aufwendigen Smartcards, zum Beispiel für Bezahlfernsehen, der Geldkarte oder dem elektronischen Reisepass, auch Maßnahmen gegen Seitenkanalangriffe. Diese verschleiern die Seitenkanalinformation während der Ausführung der Verschlüsselung, sodass die Zahl der Messkurven für einen erfolgreichen Seitenkanalangriff unpraktikabel hoch wird.

Noch lässt der Kostendruck die Hersteller im Embedded-Bereich immer wieder zu einfachen Lösungen greifen. Doch mit weiteren erfolgreichen Angriffen auf ähnliche Systeme ist zu rechnen, das Brechen von Keeloq dürfte nur der Anfang gewesen sein.

Für Keeloq selbst sind zwei Maßnahmen dringend angesagt: Statt „Security by Obscurity“ der Einsatz einer kryptologisch sicheren Chiffre wie AES statt des geknackten Keeloq und eine verbesserte Schlüsselverwaltung. Schon Letzteres würde die Verwundbarkeit des Verfahrens signifikant senken.

Auch ein längerer Seed würde den Lauschangriff erschweren, allerdings nichts an der generellen „Einfachheit“ der Extraktion der Schlüssel ändern. Microchip lässt auch bei den meisten Geräten einen 60-Bit-Seed zu, aber die OEMs scheinen ihn ungern zu nutzen, weil er den Anlernvorgang komplizierter macht. Die Autoren haben jedenfalls noch kein 60-Seed-Gerät zu Gesicht bekommen. (JS)

THOMAS EISENBARTH, TIMO KASPER

sind wissenschaftliche Mitarbeiter am Lehrstuhl für Embedded Security an der Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität Bochum

DR.-ING. CHRISTOF PAAR

ist der Inhaber des Lehrstuhls, der sich mit verschiedenen Aspekten der angewandten Kryptografie und Informationssicherheit auseinandersetzt und zu den weltweit führenden Kryptografie-Forschungsgruppen zählt.

Literatur

[1] Andrey Bogdanov; Attacks on the Keeloq Block Cipher and Authentication Systems; in: 3rd Conference on RFID Security 2007 (RFIDSec 2007); rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf

[2] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, Mohammad T. Manzuri Shalmani; On the Power of Power Analysis in the RealWorld: A Complete Break of the KeeLoq Code Hopping Scheme; Crypto 2008

[3] Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel; A Survey of Lightweight Cryptography Implementations; IEEE Design & Test of Computers – Special Issue on Secure ICs for Secure Embedded Computing; 2007

[4] Lehrstuhl für Embedded Security; www.crypto.ruhr-uni-bochum.de

[5] Tim Güneysu, Timo Kasper, Martin Novotný, Christof Paar und Andy Rupp; Cryptanalysis with COPACOBANA. To appear in „Special-Purpose Hardware for Cryptography and Cryptanalysis“ of IEEE Transactions on Computers

[6] Microchip HCS410, KeeLoq Code Hopping Encoder and Transponder; ww1.microchip.com/downloads/en/DeviceDoc/40158e.pdf

[7] Horst Görtz Institut für IT-Sicherheit; www.hgi.rub.de

[8] Paul C. Kocher, Joshua Jaffe, Benhamin Jun; Differential power analysis; Crypto ’99 Proceedings; Springer, 1999

[9] Jan Krissler, Karsten Nohl, Henryk Plötz; Chiptease; c’t 8/08; S. 80

[10] Stefan Mangard, Elisabeth Oswald, Thomas Popp; Power Analysis Attacks; Springer Science + Business Media 2007

[11] Sebastian Indesteege, Nathan Keller, Orr Dunkelmann, Eli Biham, Bart Preneel; A Practical Attack on KeeLoq; EUROCRYPT 2008, LNCS 4965, pp. 1–18; www.cosic.esat.kuleuven.be/publications/article-1045.pdf









Geodaten: SQL Server 2008 und Virtual Earth

Adressen im Web

Gerhard Völkl

Es fällt schwer, sich räumliche Beziehungen zwischen mehreren Adressen vorzustellen. Ungleich aufschlussreicher ist es, Markierungen auf einer Karte zu betrachten. Dafür müssen aus Anschriften Koordinaten werden und diese Informationen auf eine Landkarte gelangen.

Internet-Kartendienste wie Google Maps oder Virtual Earth befreiten die geografischen Informationen aus den heiligen Hallen der Vermessungsämter und brachten sie auf den heimischen PC. Mit der neuen Version 2008 des SQL Server geht Microsoft einen Schritt weiter. Der Anwender kann nun Geoinformationen lokal speichern und verarbeiten, aber leider hat die Datenbank keine Funktion, das Ergebnis auf einer Landkarte darzustellen. Hier muss der Entwickler mit einigen Zeilen Code einspringen und eine Geoanwendung erstellen.

Selbst im betriebswirtschaftlichen Umfeld ist man nicht davor gefeit, Entfernungen bestimmen oder andere geografiebezogene Berechnungen durchführen zu müssen. „Wir richten jetzt neue Haltestellen ein. Suchen Sie doch einmal alle Monatskartenabonnenten aus der Kundendatenbank heraus, die nicht weiter als 300 Meter davon weg wohnen. Die soll der Vertrieb mal anschreiben. Eine Landkarte wäre auch nicht schlecht.“ So der Chef eines Nahverkehrs-Unternehmens zum Leiter der IT-Abteilung.

Von Adressen zu Geodaten

Bevor man Geschäftsobjekte – in diesem Fall Kundeninformationen – auf einer Landkarte zeigen oder geografisch auswerten kann, brauchen sie Koordinaten. Das Zauberwort heißt hier Geocoding. Dieser Service, der für eine beliebige Adresse die Koordinaten liefert, ist einer der Bausteine von Microsofts Virtual Earth.

Die Virtual-Earth-Plattform besteht aus zwei Komponenten: dem MapPoint-Webservice (s. *iX*-Link [a]), über den Programme per SOAP-Protokoll Informationen abrufen können, und dem Virtual-Earth-Javascript-Steuerelement [b], das via Ajax Landkarten und andere Geoinformationen auf HTML-Seiten darstellt. Zur Generierung von Koordinaten für eine größere Anzahl von Objekten eignet sich der MapPoint-Webservice.

Da Virtual Earth nicht in allen Fällen kostenlos zur Verfügung steht, muss sich ein Softwareentwickler bei MapPoint anmelden [c], um den Webservice nutzen zu können. Für den Entwickler ist dies kostenlos; sobald aber jemand mit Virtual Earth Geld verdient, will Microsoft einen Anteil.

Im obigen Nahverkehr-Beispiel gibt es eine Kundentabelle *AboKunde* in einer Microsoft-SQL-Datenbank, die um eine Spalte *GeoStandort* vom Typ *geography* erweitert wurde. Eine Routine holt sich für jeden Kunden, bei dem das Feld *GeoStandort* noch leer ist, die Koordinaten per SOAP-Webservice.

In .Net ist der Zugriff auf Webservices eine relativ einfache Angelegenheit. Der Entwickler fügt in seinem Projekt eine neue Webreferenz mit der HTTP-Adresse hinzu, die er bei der Anmeldung beim MapPoint-Webservice erhalten hat; die benötigten Programmobjekte legt Visual Studio automatisch an.

Das Objekt *findService* der Klasse *FindServiceSoap* repräsentiert die Geo-

coding-Komponente MapPoint-Webservice (s. Listing 1, Zeile 2).

Als Erstes benötigt der Service die Kennung und das Passwort. Mit der Einstellung *PreAuthenticate* auf *True* kann sich das SOAP-Protokoll einige Runden bei der Kommunikation sparen, die es ansonsten nur zur Authentifizierung benötigt hätte.

Ein Objekt der Klasse *Address* steht für die Adresse, die verortet werden soll (s. Zeile 8). Je nach Land und Region benötigen die einzelnen Felder unterschiedliche Einträge. Für Deutschland haben die gewählten Attribute gut funktioniert. Genauere Beschreibungen dazu sind in der Onlinehilfe zum MapPoint-Webservice-SDK zu finden.

Der komplette Input für die Koordinatensuche ist das Objekt *mAddressSpecification*. Mit dem Attribut *DataSourceName* bestimmt der Entwickler, in welcher Datenbank bei Microsoft er suchen will. Die Methode *findService.FindAddress* in Zeile 20 startet beim Webservice die Anfrage nach der passenden Adresse und liefert ein Objekt vom Type *FindResults* zurück. Das eigentliche Ergebnis der Suche, die verlangten Koordinaten, sind in *mFindResult.FoundLocation.LatLong.Latitude* (geografische Breite) und *mFindResult.FoundLocation.LatLong.Longitude* (geografische Länge) enthalten.

Hat das Attribut *mFindResults.NumberFound* den Wert *0*, so konnte der Webservice nichts zu der Adresse finden. Interessant ist noch das Attribut *mFindResults.Score*, das zwischen *0* (die Koordinate könnte richtig sein) und *1* (Koordinaten stimmen auf jeden Fall) liegen kann und damit eine Aussage über die Genauigkeit des Geocoding angibt.

Alternativ zu der beschriebenen Vorgehensweise gibt es eine asynchrone Methode, bei der die Applikation nicht warten muss und der Service eine Methode der Anwendung aufruft, sobald ein Ergebnis da ist.

Eine Stolperfalle beim Zusammenstellen des Update-Strings ist die Methode *ToString()*. Sie verwendet im deutschsprachigen Raum standardmäßig ein Komma als Dezimaltrenner, die Funktion *STPointFromText* erwartet im WKT-String aber einen Punkt. Mit dem Argument *System.Globalization.CultureInfo.InvariantCulture* („versteckt“ in Zeile 26) kann *ToString* auf die benötigte internationale Formatierung umschalten.

Die beschriebene Routine führt die Geokodierung im Nachhinein für alle bereits erfassten Kundendaten durch. Johannes Kebeck erläutert in seinem Blog [d] eine Variante, mittels der man die Geschäftsobjekte gleich beim Erstellen oder Ändern durch einen Datenbank-Trigger mit Koordinaten versorgt kann.

Für die schnelle Darstellung geografischer Daten auf einer Landkarte ist in Virtual Earth ein Javascript-Steuerelement zuständig. Der HTML-Code (Listing 2 oben) ermöglicht einer Webseite den Zugriff auf das Control und die zusätzlich benötigten Javascript-Objekttypen.

Der Einstiegspunkt ist das *OnLoad*-Ereignis der Seite. Dies braucht lediglich die Javascript-Funktion *(GetMap())* aufzurufen, die ein Objekt vom Type *VEMap* erzeugt, um damit für die Seite den Zugriff auf die komplette Funktion von Virtual Earth zu haben.

Darstellung eigener Objekte

Der Wert *divMap* legt den Bereich (HTML-*div*-Element) auf der Webseite fest, in dem sich das Steuerelement ausbreiten kann. *LoadMap* startet die Kartendarstellung und mit *SetCenterAndZoom* legt der Entwickler fest, welche Koordinate genau in der Mitte des Kartenausschnitts liegen soll und wie nah herangezoomt wird (s. Listing 2 unten, Zeile 4).

Mit diesen wenigen Codezeilen kann man mit der Seite bereits alles das machen, was man bei Karten im Internet gewohnt ist: Zoomen, den Kartentyp auf Satellitenbilder umstellen, andere Bereiche auswählen und vieles mehr. Das ist möglich, weil das Control eigene Bedienelemente enthält und selbstständig die notwendige Kommunikation via Ajax mit dem Kartenserver durchführt.

Was jetzt noch fehlt, ist die Darstellung der Kunden aus der Datenbank. Als Behälter für die grafischen Elemente der individuellen Anwendung dienen Layer, die wie Folien übereinandergeschichtet sind.

```
myLayer = new VEShapeLayer();
myMap.AddShapeLayer(myLayer);
```

Diese beiden Befehle erzeugen ein neues Layer und fügen es zum Map-Steuerelement hinzu. Eine geometrische Figur wird von einem Objekt der Klasse *VEShape* repräsentiert. Dieses

Listing 1: Geocoding mit MapPoint-Webservice

```
 1  Dim connectionString As String = "Data Source=(local); _
    Integrated Security=SSPI;Initial Catalog=BusCompany"
 2  Dim findService As New FindServiceSoap
 3  findService.Credentials = New System.Net.NetworkCredential _
    (userId,password)
 4  findService.PreAuthenticate = True
 5  Using connection As New SqlConnection(connectionString)
 6     connection.Open()
 7     Dim command = New SqlCommand("select * from AboKunde _
       where GeoStandort is null", connection)
 8     Dim mAddress = New Address()
 9     Dim reader = command.ExecuteReader
10     While reader.Read
11        With mAddress
12           .CountryRegion = "Germany"
13           .PrimaryCity = reader("Ort").ToString
14           .PostalCode = reader("Postleitzahl").ToString
15           .AddressLine = reader("Strasse").ToString & " " & _
             reader("Hausnummer").ToString
16        End With
17        Dim mAddressSpecification = New FindAddressSpecification()
18        mAddressSpecification.DataSourceName = "MapPoint.EU"
19        mAddressSpecification.InputAddress = mAddress
20        Dim mFindResults As FindResults = findService.FindAddress _
          (mAddressSpecification) 'Synchrones Suchen
21        If mFindResults.NumberFound = 0 Then
             MsgBox("Leider nichts gefunden!")
22        Else
23           Dim mFindResult = mFindResults.Results(0)
24           Using updateConnection As New SqlConnection _
             (connectionString)
25              updateConnection.Open()
26              Dim updateCommand = New SqlCommand(String.Format _
                ("update AboKunde set GeoStandort=geography:: _
                STPointFromText('POINT ({0} {1})', 4326) _
                where id={2};", mFindResult.FoundLocation.LatLong. _
                Longitude.ToString(System.Globalization.CultureInfo. _
                InvariantCulture), mFindResult.FoundLocation.LatLong. _
                Latitude.ToString(System.Globalization.CultureInfo. _
                InvariantCulture), reader("Id").
                                           ToString), updateConnection)
27              updateCommand.ExecuteNonQuery()
28              updateConnection.Close()
29           End Using
30        End If
31     End While
32     connection.Close()
33  End Using
```

Listing 2: HTML- und Javascript-Code zum Aufruf von Virtual Earth

```
1  <script type="text/javascript"
2  src="http://dev.virtualearth.net/mapcontrol/
   mapcontrol.ashx?v=6.1">
3  </script>
```

```
1  function GetMap(){ //Startet bei OnLoad
2     myMap = new VEMap('divMap');
3     myMap.LoadMap();
4     myMap.SetCenterAndZoom(new VELatLong(49.0213 ,12.0981), 13);
5  }
```

iX-TRACT

- Um Anschriften in geografisch verwertbare Koordinaten zu wandeln, bietet Virtual Earth einen Webservice an.
- Microsofts SQL Server kann diese Geodaten speichern und mit ihnen geometrische Berechnungen durchführen.
- Ausgewählte Geodaten lassen sich via Ajax an Virtual Earth zurückgeben und auf definierten Landkarten darstellen.

Listing 3: Javascript-Funktionen der Webseite zum Abruf der Daten vom SQL Server

```
01  function ShowAsShapes(){
02     var url="./ShowAsShapesHandler.ashx"
03     DoXMLHttp(url);
04  }
05  function DoXMLHttp(url){
06     var xmlHttp=GetXmlHttp();
07     if (xmlHttp) {
08        xmlHttp.Open("GET",url,true); //true=asynchron
09        xmlHttp.onreadystatechange = function(){ //callback setzen
10           if (xmlHttp.readystate==4){ //alles okay
11              var result = xmlHttp.responseText;
12              eval(result);
13           }
14        }
15        xmlHttp.send(null);
16     }
17  }
18  function GetXmlHttp(){
19     var xmlHttp=null;
20     // Internet Explorer 6 und älter
21     try {
22         xmlHttp  = new ActiveXObject("Msxml2.XMLHTTP");
23     }
24     catch(e)
25        {
26       try {
27            xmlHttp  = new ActiveXObject("Microsoft.XMLHTTP");
28        }
29        catch(e)
30        {
31           xmlHttp  = null;
32        }
33     }
34     // Mozilla, Opera, Safari sowie Internet Explorer 7
35     if (!xmlHttp && XMLHttpRequest != 'undefined') {
36        xmlHttp = new XMLHttpRequest();
37     }
38     return xmlHttp;
39  }
```

Listing 4: ASP.Net-HTTP-Handler

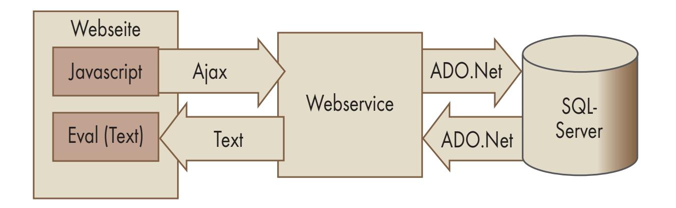
```
01  Imports System.Web
02  Imports System.Web.Services
03  Imports System.Data.SqlClient
04  Public Class ShowAsShapesHandler
05     Implements System.Web.IHttpHandler
06     Sub ProcessRequest(ByVal context As HttpContext) _
       Implements IHttpHandler.ProcessRequest
07        Dim connectionString As String = _
          "DataSource=(local); Integrated Security=SSPI; _
          Initial Catalog=BusCompany"
          context.Response.Write("var shape = null;")
08        Using connection As New SqlConnection(connectionString)
09           connection.Open()
10           Dim command = New SqlCommand("select GeoStandort.Lat, _
             GeoStandort.Long from AboKunde", connection)
11           Dim reader = command.ExecuteReader
12           While reader.Read
13              Dim pLat = CDbl(reader(0)).ToString(System. _
                Globalization.CultureInfo.InvariantCulture)
14              Dim pLon = CDbl(reader(1)).ToString(System. _
                Globalization.CultureInfo.InvariantCulture)
15              context.Response.Write("shape = new _
                VEShape(VEShapeType.Pushpin, new VELatLong _
                (" & pLat & "," & pLon & "));")
16              context.Response.Write("myLayer.AddShape(shape);")
17           End While
18        End Using
19     End Sub
20     ReadOnly Property IsReusable() As Boolean Implements _
       IHttpHandler.IsReusable
21        Get
22           Return False
23        End Get
24     End Property
25  End Class
```

kann drei verschiedene Typen speichern:
Pushpin – ein Punkt, der standardmäßig als „Stecknadel“ dargestellt wird,
Polyline – eine oder mehrere Linien, die verbunden sind,
Polygon – eine Polygon-Fläche.

Die folgenden zwei Zeilen fügen einen Punkt hinzu, der auf einer bestimmten Koordinaten in der Karte als Stecknadel erscheint. Das ist das Standardbild, das Virtual Earth verwendet, es kann aber durch eine eigene Bitmap-Datei ersetzt werden.

```
var shape = new VEShape(VEShapeType.Pushpin, ↵
                new VELatLong (49.0213, 12.0981));
myLayer.AddShape(shape);
```

Kommunikation zwischen Webseite und SQL Server mittels Webservice (Abb. 1)



Ob jetzt ein Element angezeigt wird oder das Layer alle Kunden aus der Datenbank enthalten soll, das Hinzufügen der *VEShape* funktioniert immer nach demselben Schema. Die eigentliche Schwierigkeit bei Massendaten ist nur, wie man die Koordinaten aus der Datenbank in die Javascript-Funktion der Webseite bringt.

Eine elegante Möglichkeit ist ein *XmlHttpRequest* – volkstümlicher Ajax-Call genannt – an einen Webservice, der aus der Datenbank die benötigten Informationen holt (s. Abbildung 1). Damit verursacht eine Änderung keinen Neuaufbau der Webseite. Die Aufgabe des aufgerufenen Webservice besteht darin, einen Text zu erzeugen, der alle Javascript-Befehle zum Hinzufügen der Kunden als Punkte enthält, genauso wie oben gesehen.

Dieser Text gelangt per HTPP-Protokoll wieder zurück zur Webseite und diese führt ihn dort per *Eval*-Funktion wie jedes andere Javascript aus. Das klingt vielleicht etwas kompliziert, aber es lässt sich relativ einfach mit ASP.Net im Visual Studio realisieren.

In der Beispielwebseite erledigen zwei einfache Funktionen die Anzeige der Kunden (s. Listing 3). *ShowAsShapes* stellt in Zeile 1 den URL-String für den Aufruf zusammen und *DoXMLHttp* (Zeile 3) führt danach den *XMLHttp*-Call mit dem vordefinierten *xmlHttp*-Objekt durch. Diese Routine definiert zudem noch eine anonyme Funktion, die beim Ereignis *xmlHttp.onreadystatechange* (Zeile 9) in Aktion tritt und den zurückgelieferten Text mit *eval(result)* als Javascript-Code ausführt.

Der eigentliche Ajax-Aufruf, der je nach eingesetztem Browser unterschiedlich aussehen kann, ist in der Funktion *GetXmlHttp* versteckt [e].

Damit ist die Clientseite komplett. Serverseitig reicht ein ASP.Net-HTTP-Handler mit der Dateiendung *.ashx*, der sich um den ankommenden HTML-Aufruf kümmert. Diese Art von Komponenten sind zwar praktisch, werden aber nicht häufig verwendet. Im Prinzip ist dies nichts anderes als eine normale ASP.Net-Seite ohne Oberflächenelemente. Durch die URL *./ShowAsShapesHandler.ashx* sorgt ASP.Net dafür, dass die Methode *ShowAsShapesHandler.ProcessRequest* (s. Listing 4, Zeile 4) aufgerufen wird.

Die verwendete Methode *context.Response.Write* (Zeile 7) schreibt normalerweise HTML-Text zurück. In diesem Fall aber gibt sie die benötigten Javascript-Befehle als Text zurück.

Bei großen Datenmengen ist es nicht sinnvoll, alle Elemente auf einmal zu übergeben. Eine Anpassung der Methode könnte dann so aussehen, dass vom *VEMap*-Objekt die Webseite den aktuellen Kartenausschnitt abfragt und dies über entsprechende Parameter dem zentralen ASP-HTTP-Handler mitteilt. Dieser gibt daraufhin nur die Elemente zurück, die wirklich in diesem Ausschnitt zu sehen sind.

Alternativ zur Erstellung einzelner Shapes kann Virtual Earth Dateien in den Formaten KML (Keyhole Markup Language) [f] beziehungsweise GeoRSS [g] einlesen, die Beschreibungen vieler geometrischer Elemente enthalten können.

An der gezeigten Vorgehensweise würde sich nur ändern, dass der ASP-HTTP-Handler keinen Javascript-Code erzeugt, sondern die entsprechenden Dateiformate. Merkwürdigerweise unterstützt der SQL Server 2008 keines der beiden Dateiformate durch fertige Funktionen, sondern ein alternatives Format: GML (Geografic Markup Language) der OGC [h]. GML unterscheidet sich aber nicht groß von GeoRSS; mit ein paar zusätzlichen Tags vorne und ein paar Tags hinten lässt es sich relativ leicht umbauen.

Bei Applikationen, die noch größere Datenmengen darstellen, oder wenn man das Design der Karte stärker beeinflussen will, gibt es die Möglichkeit, eigene Karten in Bilddateien zu übernehmen und diese an Virtual Earth zu übergeben. Microsoft legt die

zusätzlichen Bildkacheln (engl.: tiles) über standardmäßig vorhandene Karten.

Koordinaten auf zwei Wegen erfassen

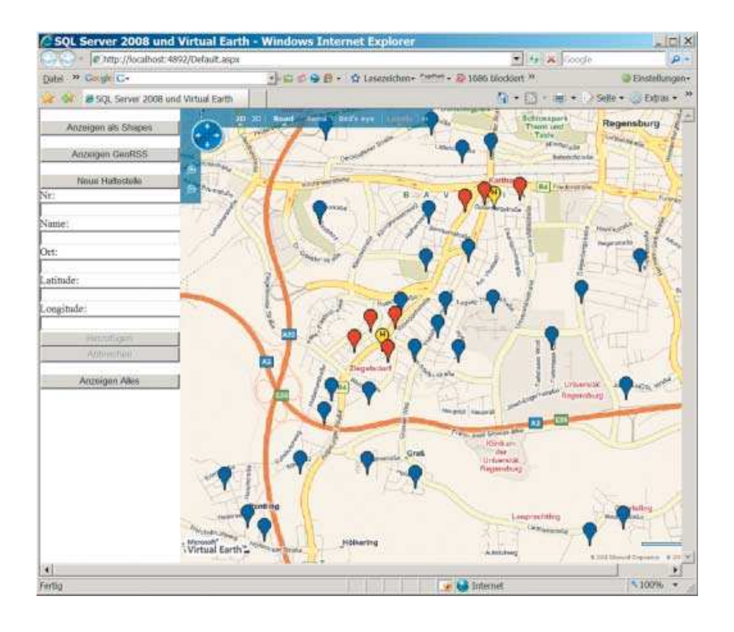
Alle Kunden haben jetzt ein Koordinatenpaar, die Mitarbeiter im Marketing können sie auch wunderbar auf einer Landkarte sehen. Aber was zur Auswertung noch fehlt, sind die Standorte der neuen Haltestellen. Da hilft Geocoding nicht weiter, denn sie haben keine Adresse mit Postleitzahl und Hausnummer. Ein Lösung dafür ist die Umkehrung des bisherigen Vorgehens: nicht Koordinaten aus der Datenbank lesen und anzeigen, sondern Koordinaten in der Landkarte anklicken und in die Datenbank schreiben.

Der grundsätzliche Ablauf mit Ajax-Aufruf und Webservice bleibt derselbe, nur der Editiervorgang erfordert einige zusätzliche Funktionen in der Webseite. Dabei ist es praktisch, dass sich Virtual-Earth-Steuerelemente in die Javascript-Funktionen der Webseite einklinken können.

```
myMap.AttachEvent("onclick", MouseClick);
```

Sobald der Entwickler in der Oberfläche den Steuerknopf zum Erfassen neuer Haltestellen gedrückt hat, klemmt sich damit die Beispielanwendung hinter den *OnClick*-Event der Map-Komponente (s. Listing 5).

Die Funktion *MouseClick* ermittelt aus dem Event-Parameter *e* die aktuelle Position in Länge und Breite, auf die der Anwender in der Map-Komponente gerade geklickt hat. Gibt es noch kein Haltestellensymbol an dieser Stelle, legt sie ein neues an, ansonsten verschiebt die Routine das vorhandene und merkt sich die Koordinaten in HTML-Eingabefeldern.



Das Endprodukt: die fertige Seite mit den Haltestellen und den benachbarten Kunden (Abb. 2)

Man kann in der Oberfläche noch einige Informationen wie Namen oder Ähnliches in HTML-Textfelder eingeben. Mit Anklicken des Steuerkopfs „Fertig mit Erfassen" führt die Webseite den Ajax-Aufruf des Webservice aus, der dann die Daten in die SQL-Datenbank schreibt. Durch die einfache Interaktion zwischen Karte und Webseite können Entwickler auf diese Weise schnell komfortable Editoren für Geoinformationen zusammenstellen.

Berechnungen und Auswertungen

Kunden und Haltestellen haben jetzt Koordinaten. Um den Chef glücklich zu machen, fehlt noch die Auswertung der geografischen Informationen. Das ist die eigentliche Stärke des SQL Server 2008. Koordinaten in zwei Datenbankfeldern speichern kann jedes Datenbanksystem, aber damit geometrische Berechnungen und Auswertungen durchzuführen ist der entscheidende Punkt. Selbst Funktionen zu schreiben, die den Abstand zwischen Punkten auf der gekrümmten

Geo-Funktionen im SQL Server

Eigenschaften, Funktion und Methoden	Beschreibung
STGeomFromText('geography_tagged_text',SRID)	erzeugt aus einem WKT-String und einer SRID ein neues Geodatenobjekt
STGeomFromWKB('WKB_geography',SRID)	erzeugt aus einem nach OCG definierten binären Byte-Array und einer SRID ein neues Geodatenobjekt
myGeoObject.STArea()	Flächeninhalt des Geodatenobjekts
myGeoObject.STAsBinary()	WKB-Repräsentation des Geodatenobjekts
myGeoObject.STAsText()	WKT-Repräsentation des Geodatenobjekts
myGeoObject.STBuffer(distance)	erzeugt ein neues Geodatenobjekt, das *myGeoObject* im Abstand von *distance* umschließt
myGeoObject.STDimension()	Anzahl der Dimensionen des Geodatenobjekts, ein Punkt hat *0*, eine Linie *1* und ein Polygon *2*
myGeoObject_1.STDisjoint(myGeoObject_2)	Methode zum Vergleich von Geodatenobjekten, liefert *1* zurück, wenn sich die beiden Objekte nicht überschneiden (verglichen wird nur, wenn beide die gleiche SRID haben)
myPoint.STDistance(otherGeoObject)	ermittelt den Abstand von einem Punktobjekt zu einem anderen Geodatenobjekt
myGeoObject.STGeometryN(n)	gibt das *n*-te Element einer *GeometryCollection* oder eines davon abgeleiteten Type, wie z. B. *MultiPoint*, zurück
myGeoObject.STGeometryType()	gibt den Typ von *myGeoObject* als String zurück
*myGeoObject_1.STIntersection(*myGeoObject_2)	erzeugt ein neues Geoobjekt, das die Überschneidung von *myGeoObject_1* und *myGeoObject_2* repräsentiert
myGeoObject_1.STIntersects(myGeoObject_2)	gibt *1* zurück, wenn sich die beiden Objekte überschneiden
myGeoColl.STLength()	Anzahl der Elemente in einer *GeometryCollection*
myGeoObject.STSrid	SRID des Geodatenobjekts
myGeoObject_1.STUnion(myGeoObject_2)	erzeugt ein neues Geoobjekt, das das Zusammenlegen der beiden Objekte repräsentiert
myGeoObject.AsGml()	erzeugt einen String, der die GML-Repräsentation (Geography Markup Language) des Geoobjekts enthält
myGeoObject.InstanceOf(geography_type)	liefert *1*, wenn *myGeoObject* vom Typ *geography_type* ist
myGeoObject.Lat	geografische Breite
myGeoObject.Long	geografische Länge
myGeoObject.ToString()	WKT-Repräsentation als String

Listing 5: Koordinaten unter dem Mauszeiger übernehmen

```
01  function MouseClick(e){
02     var x = e.mapX;
03     var y = e.mapY;
04     pixel = new VEPixel(x, y);
05     var ll = myMap.PixelToLatLong(pixel);
06     if(myCurrentHst==null){
07        myCurrentHst = new VEShape(VEShapeType.Pushpin, ll);
08        myCurrentHst.SetCustomIcon('Hst.png');
09        myLayerHst.AddShape(myCurrentHst);
10     } else {
11        myCurrentHst.SetPoints(ll);
12     }
13     document.getElementById("txtLat").value = ll.Latitude;
14     document.getElementById("txtLon").value = ll.Longitude;
15  }
```

Erde schnell berechnen, ist nicht trivial, und es muss auch nicht sein, denn das haben die Entwickler des SQL Server 2008 bereits erledigt.

```
select AboKunde.Id
from AboKunde, Haltestelle
where AboKunde.GeoStandort.STDistance ⏎
(Haltestelle.GeoStandort)<300
```

Dieses SQL-Statement ermittelt alle Kunden, die nicht weiter als 300 Meter von einer der Haltestellen weg wohnen.

In Abbildung 2 wurden die Haltestellen, die Kunden und die ausgewählten Kunden auf drei verschiedene Layers gelegt. Zur besseren Unterscheidung hat jede Selektionsmenge ein eigenes Symbol. Welche Auswertungen mit dem Datentyp *geography* möglich sind, zeigt die Tabelle „Geodatentypen im SQL Server"; alle Funktionen, die mit *ST* beginnen, sind nach OGC standardisiert. Für den Datentyp *geometry* gibt es noch einige Funktionen mehr. Falls ein Entwickler auf eine zurückgreifen muss, kann er lokal begrenzt die geografischen Koordinaten in *geometry* wandeln, die Verarbeitung durchführen und wieder zurückwandeln.

Ein Knackpunkt bei der Selektion vieler Geodaten ist die Verarbeitungsgeschwindigkeit. Mit einem speziellen Index für Geodaten, von Microsoft „Räumlichkeitsindex" genannt, kann man versuchen, positiv Einfluss zu nehmen [1]. Der SQL Server verwendet den Index nur zu Beschleunigung bestimmter Abfragen. Bei *geography*-Feldern sind dies aktuell folgende Ausdrücke:

```
geography1.STIntersects(geography2) = 1
geography1.STEquals(geography2) = 1
geography1.STDistance(geography2) < number
geography1.STDistance(geography2) <= number
```

Da sind in den kommenden Service-Releases noch einige Erweiterungen zu erwarten.

Geodatentypen im SQL Server

Basis für Geodaten im SQL Server sind die beiden Datentypen *geometry* und *geography*. Sie können verschiedene geometrische Objekte, wie einen Punkt (*Point*), einen Linienzug (*LineString*) oder eine Fläche (*Polygon*) repräsentieren, beziehungsweise eine Menge dieser Objekte (*MulitPoint, MultiLineString* oder *MultiPolygon*); die Abhängigkeit zeigt Abbildung 3 in diesem Kasten.

Eine einfache Methode, Werte in Felder mit Geodatentypen zu importieren, geht über Strings, die einen bestimmten, vom Open Geospatial Consortium (OGC) [h] definierten Aufbau besitzen. Dieser Vereinigung gehören neben Microsoft die meisten Firmen an, die sich mit dem Thema Geodaten beschäftigen.

```
insert into GeoTable (GeoCol1)
values (geography::STGeomFromText(
'POLYGON((0 0,0 8,8 8,8 0,0 0))',4326));
```

Der erste Parameter der Funktion *STGeomFromText* ist ein String, der eine Fläche mit den Koordinaten der vier Eckpunkte beschreibt (der fünfte ist die Wiederholung des ersten um ein Polygon schließen zu können). Diese Form der Darstellung ist von OGC als Well-Known Text (WKT) definiert. Der zweite Parameter Spatial Reference Identifiers (SRID) legt das verwendete Koordinatensystem fest. Und hier zeigt sich eine der Hürden beim Umgang mit Geodaten. Über die Jahrhunderte hinweg haben Wissenschaftler verschiedene Koordinatensysteme entwickelt, mit denen sie versuchen, möglichst einfach eine runde Erde auf eine ebene Landkarte abzubilden. Um noch einigermaßen den Überblick zu behalten, hat die European Petroleum Survey Group (EPSG) [i] jedem Koordinatensystem eine eindeutige Nummer, eben die SRID, verpasst.

„SRID 4326" steht für „WGS 84" (World Geodetic System 1984) eines der gängigsten Systeme, das auch die meisten GPS-Empfänger nutzen. Da der SQL Server nur Geodaten mit derselben SRID zusammen verarbeiten kann, ist es wichtig, dass alle geometrischen Objekte das gleiche Koordinatensystem haben; welches, spielt eine untergeordnete Rolle. Die Systemsicht *sys.spatial_reference_systems* liefert eine Liste der SRIDs mit einigen zusätzlichen Informationen.

Die Art des Koordinatensystems definiert den Unterschied zwischen den Datentypen *geometry* und *geography*. *geometry* unterstützt Koordinaten, die auf einer Ebene mit rechtwinkligen Achsen liegen, so wie in der Schule mit X- und Y-Achse. Da reicht zur Berechnung von Entfernungen der Pythagoras aus. Im Gegensatz dazu arbeitet *geography* mit Koordinaten, etwa geografischer Länge und Breite, die nicht in einer Ebene, sondern auf einer gekrümmten Fläche liegen. Hier sind die verwendeten Formeln für Berechnungen ungleich komplexer. Wenn Virtual Earth die Daten anzeigen soll, ist *geography* die erste Wahl, da es als Koordinaten Länge und Breite verwendet.

Die aufgeführten Objekte gibt es sowohl für die *geography*- als auch für die *geometry*-Datentypen. Die dunklen Objekttypen können instanziiert, von den hellen können andere nur abgeleitet werden (Abb. 3).

Fazit und Ausblick

Mit Virtual Earth und SQL Server 2008 können Entwickler schnell zu einer eigenen geografischen Applikation kommen, ohne dabei große Klassenhierarchien oder komplexe Protokolle studieren zu müssen. Die schlanken APIs und Funktionen sind relativ nah an der Praxis. Die Geofunktionen des SQL Servers 2008 muss man aber noch als rudimentär bezeichnen, und es bleiben zudem weitere Wünsche offen: Einbindung in OLAP-Cubes, Kartenansicht in Management Studio, bessere Indexnutzung wären wünschenswerte Inhalte für die nächsten Updates. Virtual Earth – bereits etwas länger im Einsatz – ist da auf dem richtigen Weg und erhält immer mehr Funktionen, wie etwa Routing; irgendwann gibt's wohl auch eine API für Silverlight und WPF. (WM)

GERHARD VÖLKL

ist bei einem öffentlichen Transportunternehmen für Software zuständig. Außerdem arbeitet er als Fachautor für Data Mining und Data Warehouse.

Literatur

[1] Gerhard Völkl; Stecken geblieben; Microsoft SQL Server 2008; *iX* 3/08, S. 68





Besser migrieren mit Oracles Database Replay

Was gestern war

Martin Bach



Migrationen von einer Oracle-Version zur nächsten sind in der Regel nicht trivial. Vor allem der ständig verbesserte kostenorientierte Optimizer kann unangenehme Überraschungen verursachen, die vor der Produktionsmigration gefunden sein sollten. Dabei hilft die in 11g eingeführte Replay-Funktion.

In der alten Oracle-Welt vor Einführung des kostenorientierten Optimizer (CBO) war alles noch in Ordnung: Sein wenige Regeln nutzender Vorgänger erzeugte gleichbleibende Ausführungspläne für den Datenzugriff. Dadurch konnten Entwickler sich zum Beispiel darauf verlassen, dass der Server immer einen bestimmten Index für den Zugriff auf eine Tabelle nutzt. Dabei spielte die Verteilung der Daten keine Rolle.

Dieses Konzept geriet zwangsläufig an seine Grenzen, denn die Optimierungsstrategie unterscheidet sich für Tabellen mit tausend oder einer Million Zeilen. Dies berücksichtigte der regelorientierte Optimizer nicht. Seinen Support stellte Oracle mit Version 10 ein. Sein kostenorientierter Nachfolger benutzt statt starrer Regeln statistische Informationen über Tabellen und Indizes zum Erstellen der Ausführungspläne. Da es sich aber um ein sehr kompliziertes Stück Software handelt, sind weder Fehler noch seine Evolution ausgeschlossen.

Die nicht mehr garantierte Stabilität der Ausführungspläne kann beim Umstieg von einer Oracle-Version zur nächsten zu unerwünschten Effekten führen. So kommt es vor, dass der wichtige wöchentlich laufende Report oder Batchjob nun schlechtere Ausführungspläne nutzt und 4 Stunden statt bislang 45 Minuten läuft. Solche Einbrüche lassen sich mit Oracle Database Replay verhindern. Die neue Option der Release 11.1.0 kann beliebige Datenbank-Workloads aufnehmen und wieder abspielen.

Von Oracle 10 zu 11.1 mit RAC

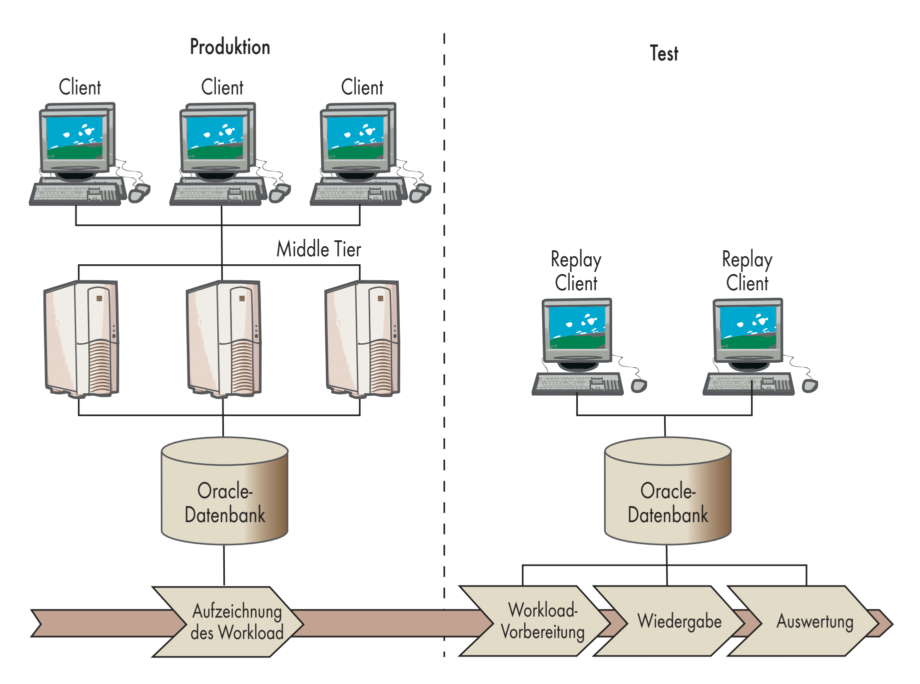
Entwickler mindern das Risiko von Migrationen oder Code-Änderungen, indem sie damit einen repräsentativen Workload des Produktionssystems aufzeichnen und unter den modifizierten Bedingungen in der Testumgebung wiedergeben. Somit fallen unliebsame Veränderungen früh genug auf. Dazu waren in der Vergangenheit einige Klimmzüge notwendig oder die Beschaffung teurer Spezialsoftware.

Ein Beispiel soll das Konzept illustrieren und den Einstieg in die Technik erleichtern: Der von Dominic Giles veröffentlichte Swingbench (dominicgiles.com/swingbench.html) erzeugt Last in Form eines Benchmarks auf einer Oracle-Datenbank 10.2.0.4 („Single Instance“) mit zwei CPUs. Anschließend soll eine 11.1.0 RAC-Enterprise-Edition diesen Workload wiedergeben, bei der beide Knoten einen Dual-Core-Prozessor zur Verfügung haben. Der Test umfasst also die Migration von 10.2. nach 11.1, von Single Instance zu RAC und von moderaten zwei CPUs zu zweimal Dual-Core-Rechnerleistung. Zum Einsatz kommen die aktuelle Version 2.3.0.376 von Swingbench, als Betriebssystem Oracle Linux 5.1 sowie Oracle 10.2.0.4 und 11.1.0.6.

Swingbench ist ein kostenfreier in Java geschriebener Lastgenerator. Der mitgelieferte Order-Entry-Benchmark simuliert einen Onlineshop: Prozesse

iX-TRACT

- Seit Version 11 bietet Oracle eine Funktion zur Wiedergabe vorher aufgezeichneter Workloads. Für das Aufzeichnen braucht man mindestens Oracle 10.2.0.4.
- Das Verfahren kann beim Umstieg auf eine neue Datenbankversion oder bei der Umstellung der Hardware helfen, da sich so rechtzeitig mögliche Performance-Einbußen oder andere Hürden identifizieren lassen.
- Beim Einsatz auf dem Produktivsystem helfen Filter bei der Auswahl der zu protokollierenden Prozesse.



Das Aufzeichnen eines Workload auf dem Produktivsystem und der Vergleich mit einer Testumgebung helfen beim Migrieren (Abb. 1).

repräsentieren Benutzer, die den Katalog anschauen, Produkte bestellen oder bearbeiten. Diese Prozesse sind in Oracles Programmiersprache PL/SQL geschrieben und laufen auf der Datenbank. Sie werden von einem Wizard konfiguriert und installiert. Vereinfacht gesagt, misst Swingbench die Transaktionen pro Sekunde, aufgeteilt nach Insert-, Update-, Delete- und Select-Anweisungen. Zudem bietet es ein hübsches GUI, das die gesammelten Daten optisch aufbereitet.

Um die Testergebnisse nicht zu beeinflussen, läuft die Software nicht auf dem Server, weshalb Oracles Instant Client 1 und eine aktuelle Java Runtime (mindestens 1.5) notwendig sind. Nach dem Download (siehe *iX*-Link) des Clients kann man ihn zum Beispiel in */opt/oracle/instantclient* entpacken. Wichtig ist, auch die später benötigte WRC-Option (Workload Replay Client) herunterzuladen und zu installieren. Workload Replay Clients sind zur Wiedergabe der Last auf dem Zielsystem erforderlich. Zur Zeit der Erstellung dieses Artikels waren sie jedoch nicht für Windows verfügbar. Die Umgebungsvariablen *PATH* und *LD_LIBRARY_PATH* sollten */opt/oracle/instantclient* enthalten.

Swingbench sollte ebenfalls unterhalb von */opt/oracle* liegen, zum Beispiel in */opt/oracle/swingbench_v23*. Seine Steuerung übernimmt eine Konfigurationsdatei. Für Linux ist dies *swingbench.env*, Windows-Benutzer verwenden *swingbenchenv.bat*. Dort passt man die Umgebungsvariablen an den Instant Client an.

Benchmark per Wizard parametrieren

Für Swingbenchs Order-Entry-Benchmark erfragt der Wizard *oewizard* die nötigen Parameter: den Benutzer, unter dem der Benchmark läuft, den Speicherort für die Daten und so weiter. Er erzeugt außerdem die „Spieldaten“ des Benchmark. Hat der Wizard seine Arbeit beendet, was je nach Datenvolumen einige Minuten dauern kann, muss das Datenbankschema (also Tabellen, Indizes, Stored Procedures und so weiter) exportiert werden. Dies geht am einfachsten mit *exp* oder *expdp*, zum Beispiel:

```
expdp system@ora10 directory=data_pump_dir \
 logfile=exp_soe_080429.log \
 dumpfile=exp_soe_080429.dmp schemas=soe
```

Dieses Kommando sichert das Order-Entry-Schema *SOE* im Directory-Objekt *DATA_PUMP_DIR*. Der Export der Daten schafft identische Voraussetzungen in beiden Datenbanken.

Oracle hat das Mitschneiden eines Workload in 10g erst mit dem dritten Patchset (10.2.0.4) ermöglicht, frühere Versionen scheiden hier aus. Damit es funktioniert, muss der Parameter *pre_11g_enable_capture* auf „true“ stehen, was zum Beispiel ein Aufruf des Skripts *$ORACLE_HOME/rdbms/admin/wrrenbl.sql* unter der Benutzerkennung *system* oder *sys* erledigt. Eine weitere Voraussetzung ist ein Directory-Objekt, das Metainformation über den aufgezeichneten Prozess speichert. Da es bei aufwendigen Tests schnell anwachsen kann, sollte vor dem Beginn der Aufzeichnung genügend freier Plattenplatz vorhanden sein.

Zur Steuerung der Aufnahme stehen zwei Methoden zur Verfügung: Enterprise Manager DB Console und PL/SQL-Pakete. Dokumentation zu beiden findet sich unterotn.oracle.com im „Performance Tuning Guide“ unter „Real Application Testing“. Da der Autor ein Verfechter der Kommandozeile ist, seien hier die APIs verwendet. Die Vorgehensweise in DB Console ähnelt dem im Folgenden Beschriebenen.

Vor dem Start des Benchmarks sollten Sicherheitsmaßnahmen stehen. Zum einen ist es ratsam, die Datenbank herunterzufahren, um alle laufenden Transaktionen zu beenden. Dies lässt sich jedoch häufig nicht machen, wenn es sich um eine Produktionsdatenbank handelt. Weiterhin wäre es wünschenswert, lediglich die aufzunehmenden Prozesse auf dem Server zu erlauben, was sich aus ähnlichen Gründen schwierig gestalten dürfte.

Protokoll mit Filtern einschränken

Ein möglicher Weg aus dem Dilemma sind Filter, die Ein- und Ausschlusskriterien definieren. Das folgende Beispiel protokolliert nur Prozesse des Benutzers *SOE*:

```
BEGIN
 DBMS_WORKLOAD_CAPTURE.ADD_FILTER (
              fname => 'nur_soe_prozesse',
              fattribute => 'USER',
              fvalue => 'SOE');
END;
```

Auf dem zweiten PC startet man nun den nach den eigenen Vorstellungen parametrierten Swingbench. Der Autor verwendete 75 Benutzersitzungen, die übrigen Einstellungen entsprachen mit Ausnahme des Verbindungsdeskriptors (der auf die 10.2-Datenbank zeigt) den Voreinstellungen. Für den Benchmark ist nun alles vorbereitet, er läuft jedoch noch nicht.

Um den Mitschnitt auf Seiten der Datenbank zu starten, bedarf es folgender Anweisung:

```
BEGIN
  DBMS_WORKLOAD_CAPTURE.START_CAPTURE (
      name => 'iX_test_080429',
      dir => 'CAPTURE',
      duration => 600);
END;
```

Sie lässt den Aufnahmeprozess namens „iX_test_080429“ für 600 Sekunden laufen, der alle erzeugten Dateien in das Verzeichnisobjekt *capture* speichert. Sobald das Kommando ausgeführt ist, startet man den Swingbench-Benchmark auf der zweiten Maschine.

Nach dem Ende des Mitschnitts enthält der View *DBA_WORKLOAD_CAPTURES* alle Informationen über Status und Verlauf. Falls gewünscht, kann nun das AWR (Automatic Workload Repository) exportiert werden, mit dessen Hilfe sich bei der abschließenden Analyse Vergleiche anstellen lassen:

```
BEGIN
  DBMS_WORKLOAD_CAPTURE.EXPORT_AWR \
    (capture_id => 1);
END;
```

Hier ist die Capture-ID durch die des Testlaufs zu ersetzen, entnommen aus *DBA_WORKLOAD_CAPTURES*.

Abschließend erzeugt die Prozedur *REPORT* einen Bericht mit einigen relevanten Daten zum Testlauf (siehe Listing 1):

Die Wiedergabe erfolgt in fünf Schritten:
– Kopieren der Rohdaten auf das Zielsystem
– Nachbearbeitung der Rohdaten auf dem Zielsystem
– Vorbereitung des Zielsystems auf die Wiedergabe
– Wiedergabe mittels der Workload Replay Clients
– Analyse und Interpretation

Daten auf das Zielsystem kopieren

Vor dem Wiedergeben der Aufnahme auf dem Zielsystem muss man sie dort nachbearbeiten. Dazu ist der Inhalt von */home/oracle/capture* in ein gemeinsam genutztes Verzeichnis (NFS-Mount/OCFS2 oder Ähnliches) zu kopieren. Oracle empfiehlt, die aufwendige Nachbearbeitung nicht auf der Produktionsdatenbank durchzuführen.

Listing 1: Report des Testlaufs

```
DECLARE
  cap_id        NUMBER;
  cap_rpt       CLOB;
BEGIN
  cap_id  := \
   DBMS_WORKLOAD_CAPTURE.GET_CAPTURE_INFO(dir => 'CAPTURE');
  cap_rpt := \
   DBMS_WORKLOAD_CAPTURE.REPORT(capture_id => cap_id,
         format => DBMS_WORKLOAD_CAPTURE.TYPE_TEXT);
  dbms_output.put_line(cap_rpt);
END;
```

Jetzt ist auch der richtige Zeitpunkt das SOE-Schema in die Zieldatenbank zu bewegen. Dazu kopiert man die vorhin erzeugte Exportdatei in ein Verzeichnis auf dem Zielsystem, im Beispiel *DATA_PUMP_DIR*, das auf */home/oracle/admin/$ORACLE_SID/dpdump* zeigt, gefolgt von einem Aufruf von *impdp*:

```
impdp directory=data_pump_dir \
  dumpfile=exp_soe_080429.dmp \
  logfile=import_soe_080429.log schema=soe
```

impdp meldet zwar einen Fehler, weil der während des Imports angelegte Benutzer *SOE* kein Ausführungsrecht für

Listing 2: Replay-Bericht erstellen

```
DECLARE
  cap_id        NUMBER;
  rep_id        NUMBER;
  rep_rpt       CLOB;
BEGIN
  cap_id := DBMS_WORKLOAD_REPLAY.GET_REPLAY_INFO(dir => 'CAPTURE');
  /* Nur Information zum letzten Testlauf */
  SELECT max(id)
  INTO   rep_id
  FROM   dba_workload_replays
  WHERE  capture_id = cap_id;
  rep_rpt := DBMS_WORKLOAD_REPLAY.REPORT(replay_id => rep_id,
                         format => DBMS_WORKLOAD_REPLAY.TYPE_TEXT);
END;
```

DBMS_LOCK hat, läuft jedoch durch. Den Fehler behebt ein *grant execute on dbms_lock to soe*.

Nun fehlt nur noch das Directory-Objekt zum Speichern der Aufnahme, das der Befehl

```
create directory capture as \
'/media/nfs_mounts/oracle/capture'
```

anlegt. Die Verarbeitung der rohen Daten erfolgt durch folgendes Kommando auf der RAC-Datenbank:

```
BEGIN
 DBMS_WORKLOAD_REPLAY. ⤶
                      PROCESS_CAPTURE \
   (capture_dir => 'CAPTURE');
END;
```

Somit sind die Voraussetzungen zur Wiedergabe erfüllt.

Aktuellen Zustand sichern

Bevor es nun aber an die eigentliche Wiedergabe gehen kann, sind noch weitere Schritte erforderlich. Zum einen kann es nötig sein, die Systemzeit mit der Aufnahme zu synchronisieren. Sonst entstehen möglicherweise Datenabweichungen, beispielsweise durch *INSERT*-Befehle, die *sysdate* verwenden. Außerdem könnte es erforderlich sein, Referenzen zu externen Systemen zu bearbeiten, schließlich soll das Testsystem nicht über Datenbank-Links auf andere Produktionssysteme zugreifen. Unter diese Kategorie fallen auch externe Tabellen, Verzeichnisobjekte und verwendete Streams. Im hier vorgestellten braucht man sich darum nicht zu kümmern. Auf all diese Fälle einzugehen, sprengte den Artikelumfang. Es sei hier auf das Performance-Tuning-Handbuch zu Oracle 11g verwiesen.

Als Nächstes sollte man einen Restore Point definieren, auf den sich die Datenbank bequem mittels *Flashback Database* [1] zurücksetzen lässt. Dies ist besonders für die Durchführung von Testserien nützlich.

Der Aufruf von *DBMS_WORKLOAD_REPLAY.INITIALIZE_REPLAY* bereitet die Datenbank auf die Wiedergabe vor und stellt notwendige Metadaten im Data Dictionary bereit:

```
BEGIN
 DBMS_WORKLOAD_REPLAY.INITIALIZE_
REPLAY (
    replay_name => 'iX_replay_080429_001',
    replay_dir => 'CAPTURE');
END;
```

Oracle erlaubt es weiterhin, die Wiedergabeparameter zu beeinflussen. Die nützlichsten mit *DBMS_WORKLOAD_REPLAY.PREPARE_REPLAY* konfigurierbaren Optionen sind:

– Reihenfolge der Commit-Anweisungen: normalerweise spielt Oracle alle Transaktionen in der Reihenfolge der Aufnahme ab. Dies lässt sich abstellen, sodass die Transaktionen in der Reihenfolge ihrer Beendigung wiedergegeben werden, was zu Datenabweichungen führen kann.

– Die Option „Think Time“ passt die Dauer der Wiedergabe an die der Aufnahme an. Dies ist nützlich, sollte das Abspielen wesentlich länger dauern als das Aufzeichnen.

Der oben genannte Aufruf von *DBMS_WORKLOAD_REPLAY.PREPARE_REPLAY* hat die Datenbank darauf vorbereitet, Verbindungen von WR-Clients anzunehmen, die die eigentliche Wiedergabe des Workload übernehmen. Ähnlich Swingbench sollten sie nicht auf den Datenbankservern laufen. Wie bei der Aufnahme übernimmt der Instant Client 11 die Steuerung des WRC. Am einfachsten ist es, auf den Wiedergabe-PCs ein Oracle-Konto anzulegen, das die primäre Gruppe *oinstall* und die weiteren Gruppen *dba* und *users* zugeordnet bekommt.

Vergleichsdaten erzeugen und auswerten

WRC benötigt Zugriff auf die bearbeiteten Capture-Daten. Im Beispiel bindet man dazu das NFS-Verzeichnis an die PCs an. Mit dem Kalibrierungsmodus lässt sich die Zahl erforderlicher WRCs ermitteln:

```
wrc system@ora11 MODE=calibrate  \
 REPLAYDIR=/media/nfs_mounts/oracle/capture/
```

Die Ausgabe dieses Kommandos enthält unter anderem:

```
...
Recommendation:
Consider using at least 2 clients divided among 1
CPU(s).
...
```

Im dargestellten Szenario sind also zwei WRC-Sitzungen nötig, die man jeweils durch

```
wrc system/sys@ora11 \
 REPLAYDIR=/media/nfs_mounts/oracle/capture/
```

in Betrieb nimmt. Sind alle WRC-Sitzungen zur Datenbank aufgebaut, startet der Aufruf von *DBMS_WORKLOAD_REPLAY.START_REPLAY()* die Wiedergabe. Die WRCs quittieren dies mit „Replay started“ und der Uhrzeit. Nach dem Ende des Wiedergabeprozesses sollte das AWR ein weiteres Mal exportiert werden, wenn man die gesammelten Snapshot-Information beispielsweise für Testserien behalten möchte.

Nach dem Ende des Wiedergabeprozesses kann es endlich an den Vergleich gehen. Er sollte hoffentlich Verschlechterungen der Ausführungspläne oder Ähnliches aufdecken. Analog zur Vorgehensweise bei der Erstellung des Capture-Berichts gibt es eine Funktion zur Erstellung des Replay-Berichts (siehe Listing 2). Alternativ lässt sich der Report im HTML-Format erzeugen, was der Parameter *DBMS_WORKLOAD_CAPTURE.TYPE_HTML* veranlasst.

Dieser Bericht erlaubt es, detaillierte Schlüsse über den ursprünglichen Workload im Vergleich mit der Wiedergabe zu ziehen. Mithin ist es möglich, Korrekturen auf der Wiedergabedatenbank vorzunehmen und mittels *Flashback Database* einen weiteren Test durchzuführen. (ck)

MARTIN BACH

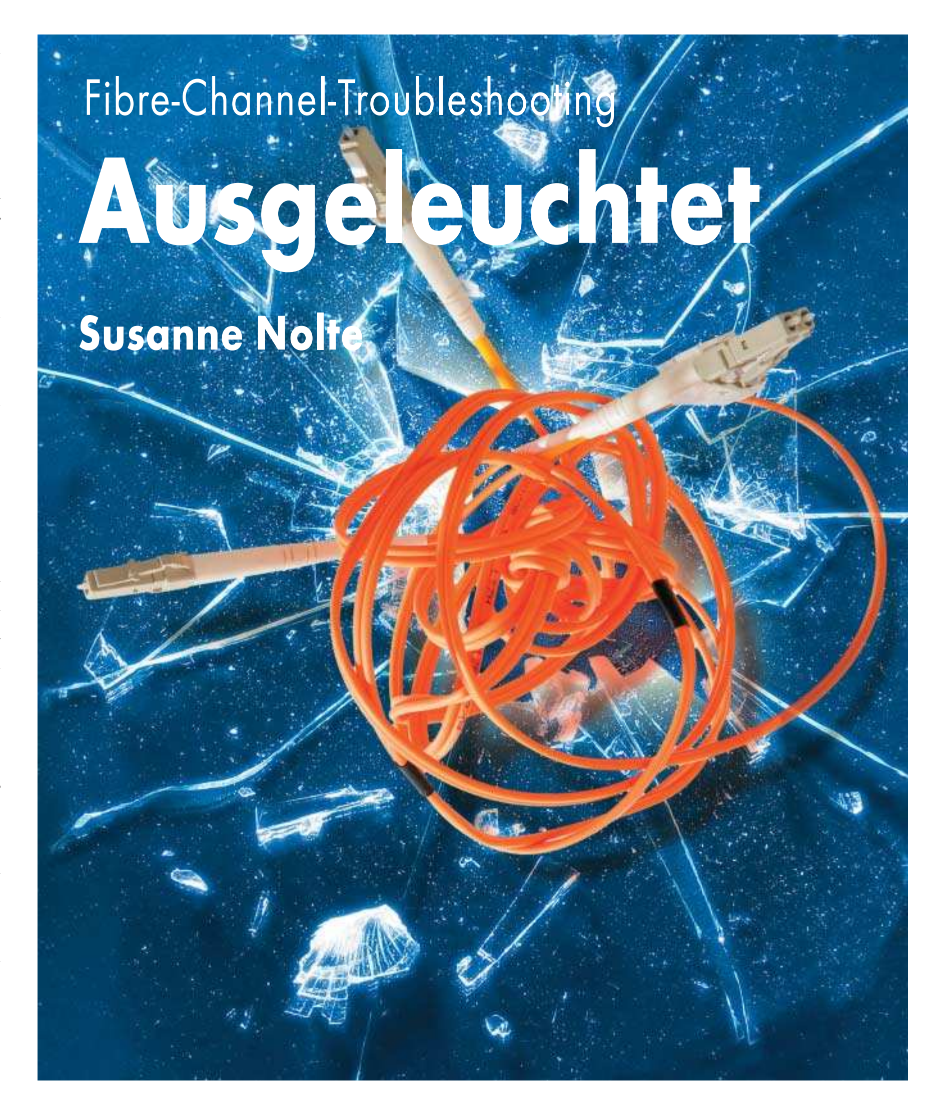
ist Oracle-Datenbank-Administrator und arbeitet als Consultant mit Schwerpunkt Oracle Real Application Cluster, Hochverfügbarkeit und Disaster Recovery in Brighton/England.

Literatur

[1] Andrea Held; Datenbanken; Oracle-Flashback; Gute alte Zeiten; *iX* 10/05, S. 150







Fibre-Channel-Troubleshooting

Ausgeleuchtet

Susanne Nolte

Serveradmins, die ihre Schützlinge bisher nur mit internen oder direkt angeschlossenen Festplatten oder Tapes versehen haben, schrecken oft davor zurück, den Massenspeichern ein eigenes Netz zu gönnen – zumal, wenn es aus Fibre Channel bestehen soll. Dabei ist ein FC-Netz nicht schwerer zu handhaben als ein Ethernet.

Was für Ethernet gilt, gilt auch für Fibre Channel (FC): Grundsätzlich fängt das Troubleshooting nicht erst bei der Fehlersuche an, sondern beim Fehlervermeiden. Den größten Teil der Fehlersuche spart man sich dadurch, dass man Schritt für Schritt vorgeht und nach jedem einzelnen Schritt das Ergebnis prüft. Wie beim Aufbau jedes Netzes beginnt man auch beim SAN mit der Verkabelung von Port zu Port.

Nach dem Verkabeln sollte man sich auf jedem Gerät per Management-Tool einloggen – also per „Elementen-Manager“, Web-GUI, *telnet*, SSH oder seriell – und die Rückmeldungen der FC-Controller und -Switches prüfen. Die wichtigsten Hinweise liefern in diesem Stadium die Switches: Schon beim Verkabeln zeigen sie – manchmal mit etwas Verzögerung – durch grüne und rote Kontrollleuchten an, ob eine Verbindung an den einzelnen Ports besteht. Mit welcher Geschwindigkeit sie arbeiten und welche Topologie sie benutzen, verrät ein Blick in das Web-GUI.

Die Fibre-Channel-Welt kennt drei Topologien: Point-to-Point, Arbitrated Loop (AL) – ähnlich dem Token Ring – und Fabric, also ein vermaschtes Netz. In der Praxis sind Fabric und Point-to-Point miteinander verschmolzen, da Letzteres beim FC ohne Crossover-Kabel auskommt und in der Fabric jede Port-zu-Port-Verbindung als Point-to-Point gilt. Heutige Fibre-Channel-Komponenten unterstützen in der Regel sowohl die Arbitrated Loop als auch die Fabric, daher lauert hier die erste größere Falle.

Grundsätzlich sollte man sich vorher für eine Topologie entscheiden und diese bei allen Geräten einstellen. Am einfachsten erkennt man das an den zugewiesenen Port-Typen: In einer Loop sind sie als L_ (Loop), FL_ (Fabric Loop) oder NL_Ports (Node Loop) deklariert, in der Fabric heißen die Ports der Endgeräte N_Ports und die des Switches F_Ports (Fabric) bei Anschluss eines Endgeräts, E_Port (Extention) bei Verbindung mit einem anderen Switch. Solange kein Gerät angeschlossen ist oder der Switch keine Topologie aushandeln kann, sind sie in der Regel als U_Ports (Universal) ausgewiesen.

Besitzen alle Ports die richtigen Typen und leuchten alle Lampen grün, kann man sich außerdem über das Web-GUI in der Detailansicht der Ports vergewissern, ob sie Pakete senden und empfangen. Auch die Storage-Controller geben Auskunft über Aktivität, Geschwindigkeit und zugewiesenen Typ (Topologie) der Ports. Dazu zieht man in diesem Stadium das Firmware-Setup zurate.

Stecker verwechsle dich

Besteht zwischen zwei Ports keine Verbindung, kann das mehrere Gründe haben. Neben an den Endpunkten unterschiedlich eingestellten Topologien und Geschwindigkeiten gehören vertauschte Stecker zu den häufigsten: Im SAN gebräuchliche Glasfaserkabel oder Lichtwellenleiter (LWLs) besitzen an jedem Ende zwei sogenannte LC-Stecker für das SFP- (Small Form Factor Pluggable) oder XFP-Interface (10 Gigabit Small Form Factor Pluggable), bestehend aus Einzelfaser-Keramikhülsen [1].

Da bei Fibre Channel über LWL zweiadrige Kabel üblich sind, hält oft eine Duplexklammer die beiden Stecker eines Kabelendes zusammen. Viele Kabel besitzen, für den Fall, dass die Klammern fehlen oder entfernt werden, Farbmarkierungen. Jede Farbe – häufig weiß und gelb – markiert eine Faser (siehe Abbildung 1). Andernfalls ist Probieren angesagt.

Unangenehmer und meist zeitraubender sind defekte Glasfasern im Kabel. Zwar ist der erlaubte Biegeradius von LWLs ausgesprochen klein – Hersteller geben das Zehnfache des Außendurchmessers an –, doch genügt schon ein kurzes Hängenbleiben des Kabels am Rack, an einer Kante oder Ecke, damit eine Faser bricht. Herausfinden kann man das nur auf zwei Wegen: Probieren oder Testen. Im ersten Fall tauscht man das suspekte Kabel gegen ein anderes, im zweiten zieht man – wenn vorhanden – einen Optical Time Domain Reflectometer (OTDR) hinzu, mit dem man die Faser durchmisst.

Schuld an einem toten Link können auch falsche oder defekte Transceiver sein: Durchgesetzt haben sich beim Fibre Channel inzwischen die modularen Ports; nur bei den FC-HBAs (Host Bus Adapter) finden sich, vor allem bei älteren Modellen, fest eingebaute Transceiver. Der Haken: In den austauschbaren Port-Modulen sitzen Sender und Empfänger (Receiver) für die jeweilige Übertragungstechnik. Dadurch sind zwar FC-I/O-Controller und Switches nicht an ein bestimmtes Transportmedium gebunden – auf kurzen Strecken meist Multimode-LWLs, bei langen Singlemode-Fasern. Zumindest aber die an beiden Enden verwendeten Transceiver müssen zum Kabel (Mode und Wellenlänge) passen – und vom Gerät unterstützt werden.

Nicht immer der kürzeste Weg

Holt man ältere, etwa für 2 GBit/s spezifizierte Transceiver aus dem Schrank und verbindet sie mit zum neuen Gerät mitgelieferten 4-GBit/s-Transceivern, kann das ebenfalls Disconnects verursachen. Hier gilt es zumindest darauf zu achten, dass die Transceiver an beiden Enden eines Kabels dieselbe Geschwindigkeit, das heißt Frequenz, unterstützen – die Controller und Switches schalten gegebenenfalls automatisch herunter.

Ist der Server mit dem Speichersystem – etwa zum Testen – direkt, also Point-to-Point, verbunden und findet Letzteres nicht, sollte man zuerst wie gewohnt die Kabel und Stecker sowie die eingestellte Topologie und Geschwindigkeit überprüfen. Um zu sehen, ob die Fibre-Channel-Kommunikation funktioniert, kann man an beiden Enden die Topologie und Geschwindigkeit auf „auto“ einstellen. Haben sich beide Systeme auf eine Topologie und eine Geschwindigkeit geeinigt, steht zumindest die Verbindung. Wenn die verwendete Konfiguration – OS, Treiber, Firmware, Hardware – als getestet in den Kompatibilitätslisten steht und nichts weiterhilft, bleibt einem wahrscheinlich nichts anderes übrig, als sich einen FC-Switch dazuzuleihen und mit dem ganzen Prozedere von vorne zu beginnen.

Erst wenn alle Port-zu-Port-Verbindungen stehen, kann man sich an die geräteübergreifenden Verbindungen setzen. Auf den Servern sollte man auf jeden Fall zu den FC-HBA-Treibern auch die HBA-Tools respektive -Agents der Hersteller installieren.

Im Unterschied zum Firmware-Setup greifen sie über die OS-Treiber auf die HBA-Firmware zu, können aber den HBA im laufenden Server-Betrieb konfigurieren. Die GUI-Versionen stellen die vernetzten FC-Devices darüber hinaus grafisch dar. Mit ihnen lässt sich am einfachsten die FC-Netz-Topologie überprüfen. Zudem sollten für den HBA dann alle Storage-Controller sichtbar sein.

Unter Linux empfehlen sich zusätzlich die *sg3-utils* respektive *scsi-tools*. Da alle Fibre-Channel-Geräte auf der Serverseite als SCSI-Geräte erscheinen, kann man mit ihnen kontrollieren, ob der Kernel neue *sg*-Devices (SCSI Generic) gefunden hat.

Für Bandlaufwerke und Tape Libraries halten FC-HBAs eine zusätzliche Hürde bereit. Oft besitzen sie in den Tiefen des Firmware-Setups eine Option „Tape Support“, die man mitunter erst einschalten muss.

Ist alles korrekt verkabelt und leuchten alle Lampen grün, kann aber der Server ein Storage-System respektive seinen Controller nicht sehen, sollte man auf dem Switch prüfen, ob nicht aus einer früheren Testkonfiguration noch ein Hard-Zoning übrig geblieben ist.

Im Unterschied zum – recht unsicheren – Soft-Zoning, bei dem der Namensdienst den Servern die Auskunft über Geräte verweigert, die in anderen Zonen liegen, ist für das Hard-Zoning die Switch-Firmware zuständig. Ordnet man mehrere Ports einer Zone zu, unterbricht sie die Kommunikation zwischen ihnen und allen anderen Ports außerhalb der Zone, meist durch Deaktivieren der Verbindungen im internen Crossbar-Switch.

Gut versteckte Beschränkungen

Da ein solches Zoning Know-how voraussetzt, beschränken die Hersteller den Zugriff auf das Zonen-Management gern auf das Command Line Interface (CLI) oder umfangreiche Management-Werkzeuge. Dadurch sind im Web-GUI die Zonen schlicht unauffindbar, was zur stundenlangen Fehlersuche an den falschen Stellen führen kann.

Will man dagegen ein Zoning auf den Switches erst einrichten, wäre dies ein geeigneter Zeitpunkt, da die Storage-Controller für die Server schon sichtbar sind und sich das richtige Zuordnen mit den HBA- oder *scsi-tools* verifizieren lässt, ohne dass wie aus dem Nichts erscheinende Volumes Mensch und Maschine verwirren.

Steht die Verbindung zu den RAID-Controllern, kann man sich mit den Volumes beschäftigen. Normalerweise hat man sich während der Planung ausführlich mit der gewünschten Kapazität beschäftigt, doch sollte man auch die Performance berücksichtigen.

Die drei Kandidaten für Engpässe hinter dem Server sind die FC-Leitung mit ihren 2 oder 4 GBit/s, ein Controller mit zu langsamem Prozessor und die RAID-Sets. Falls man nicht gerade RAID-1-Sets benötigt, sollte man die Plattenanzahl so wählen, dass die Platten zusammengerechnet – unter Berücksichtigung von Paritäts- und dedizierten Hot-Spare-Platten – den Fibre-Channel-Durchsatz nicht unterbieten; außerdem sollte man RAID 6 ohne Hardware-Beschleunigung meiden.

Erhält man dadurch mehr Kapazität als gewünscht, kann man bei den meis-

iX-TRACT

- Wie immer ist das A und O der Fehlersuche auch beim Fibre Channel die systematische Vorgehensweise.
- Zu den häufigsten Fehlerquellen im SAN zählen defekte Kabel und falsch konfigurierte Ports.
- Die Management-Schnittstellen der Fibre-Channel-Switches und -Controller erlauben es, die Fehler räumlich einzugrenzen.

Einmal mit Duplexklammer, einmal ohne. Für den Fall, dass die Klammern fehlen oder abbrechen, besitzen viele Kabel Farbmarkierungen. Hier ist jeder Ader eine Farbe zugeordnet (Abb. 1).

ten Disk-Systemen die RAID-Sets in mehrere Volumes oder LUNs unterteilen. Zu viele Mitglieder sollte ein RAID-Set aber nicht beinhalten, da das auf Kosten der Ausfallsicherheit geht. Als Daumenregel gilt: Die Wahrscheinlichkeit eines RAID-Ausfalls sollte geringer als die des Ausfalls einer einzelnen Festplatte sein. Die Zahl, die sich daraus ergibt, hängt stark von der Ausfallwahrscheinlichkeit AFR (Annual Failure Rate) der Platten ab: Je geringer die AFR, desto größer kann das RAID-Set sein.

In der Regel können Disk-Systeme die RAID-Sets im Hintergrund aufbauen, während man die Volumes oder LUNs einrichtet. Auch hier empfiehlt sich die vorherige Lektüre des Handbuchs, da jeder RAID-System-Hersteller ein anderes Konzept und andere Begriffe verwendet, mit denen es sich vertraut zu machen gilt. Das gilt auch und vor allem für die Zuordnung von LUNs zu bestimmten Servern: In der Fibre-Channel-Nomenklatur heißt das LUN-Masking, einzelne Hersteller nennen es LUN-Mapping – worunter andere wiederum das Verknüpfen von LUNs und Volumes verstehen – oder Filtering. Auf jeden Fall sollte man die LUNs dem jeweiligen Server fest zuordnen, um konkurrierende Zugriffe zu vermeiden.

Dies wäre auch der richtige Zeitpunkt, wenn man Inband-Storage-Virtualisierer einsetzen will. Dazu weist man der Maschine, auf der der Virtualisierer läuft, die LUNs zu, richtet dort die Volumes ein und gibt sie an die Server weiter.

Zu tief ins Glas geschaut

Wer jemals ein Fibre-Channel-Netz aufgebaut hat, hat wahrscheinlich sämtliche der folgenden Resultate kennengelernt: Der Server sieht die Volumes gar nicht, gleich mehrfach oder ein anderer Server findet sie. Der letzte Fall sollte durch vorheriges Hard-Zoning und LUN-Masking ausgeschlossen sein. Wenn nicht, gilt es, beides zu überprüfen.

Findet der zugewiesene Server die Volumes nicht, kann die „lange Leitung“ (Reaktionszeit) der HBA-Firmware oder der Treiber dafür verantwortlich sein. Ersterer kann man im Setup oder den HBA-Tools mit einem „Scan Fabric“ auf die Sprünge helfen. Sollte danach beim Betriebssystem immer noch nichts angekommen sein, hilft nur eins: Treiber-Module entfernen und neu laden, sofern möglich. Was unter Linux ein *modprobe –r*

<module> und *modprobe <module>* erledigt, kann man unter Windows im Geräte-Manager mit Deaktivieren/Aktivieren erreichen.

Harmlos, aber unschön ist es, wenn ein Server scheinbar zu tief ins Glas geschaut hat: Zumindest weiß man, dass die redundanten Pfade ihren Dienst tun. Ist sowohl der Server als auch das Storage-System doppelt verkabelt, Letzteres eventuell sogar mit zwei Controllern ausgestattet, kann es auch zu Vier- oder Achtfachsichtungen kommen. Um herauszufinden, auf welcher Seite der Schuldige sitzt – ob der Server tatsächlich doppelt sieht oder sich das Storage-System doppelt zeigt –, kann man mit den HBA- oder SCSI-Tools nachprüfen, wie viele Storage-Controller der Server über welche SCSI-Kanäle findet.

Sieht der Server auf einem SCSI-Kanal einen Controller doppelt, liegt es an dessen Doppelleitung, sieht er beide Controller auf einem Kanal, ist die Controller-Konfiguration schuld daran. Viele RAID-Systeme beispielsweise arbeiten bei doppelter Controller-Bestückung automatisch im Fail-over-Modus oder sind bereits so vorkonfiguriert, bei anderen muss man es erst einstellen, so die Controller nicht je eigene Server bedienen sollen. In diesem Fall muss man darauf achten, dass die Controller auch unterschiedliche Volumes verwalten (können).

Bei manchen Geräten blendet die Firmware im Failover-Modus einen Controller komplett aus, wieder andere erlauben es, pro Volume einen Primär- und einen Sekundär-Controller zuzuweisen. Eine Ausnahme bilden die kleinen Clariion-Systeme von EMC, die nur über eine externe Path-Manager-Software für Windows ein Failover beherrschen. Die ATA- und SATA-Beasts von Nexsan verteilt die Platten auf beide Controller und kennen daher überhaupt kein Controller-Failover. Will man sich also böse Überraschungen ersparen, bleibt einem wohl nichts anderes übrig, als sich bereits vor der Anschaffung neuer Disk-Subsysteme mit deren Failover-Konzepten zu beschäftigen und danach das für die eigenen Anforderungen passende auszuwählen.

Und alles von vorne

Hat man sich beim Konfigurieren verzettelt oder wurde das (Test-)System verkonfiguriert geliefert, kann man sich viel Arbeit sparen, indem man auf die Werkseinstellungen zurückgreift. Vor diesem Schritt sollte man aber auf jeden Fall das Handbuch konsultieren und sich Account-Name, Passwort, IP-Adressen und Baudrate der seriellen Schnittstelle in den Werkseinstellungen notieren, um sich nicht auszusperren. Nach dem Reset sind Passwort und IP-Adressen die ersten Einstellungen, die es zu ändern gilt.

Ist das Speichernetz bereit, kann man mit dem Partitionieren und Formatieren beginnen. Allerdings lauern auch hier noch Stolpersteine: Bricht das Formatieren oder die Datenübertragung ab, liegt es seltener an einer instabilen als an einer zu langsamen Leitung. Deshalb sollte man möglichst die Performance überprüfen, bevor einem dieses Missgeschick bei der Übertragung der Produktivdaten widerfährt. Unter Linux und Unix-Derivaten kann man das mit Bordmitteln wie *time dd* bewerkstelligen, unter Windows kann man auf *iozone* oder Ähnliches zurückgreifen. Die Performance sollte der zuvor errechneten entsprechen.

Nach dem Formatieren geht es daran, die Stabilität zu testen, etwa, indem man mehrfach große Mengen von Testdaten hin und her schaufelt. Grundsätzlich zeichnet sich Fibre Channel seit Jahren durch eine hohe Stabilität aus, nach dem Motto: Wenn eine FC-Verbindung erst einmal steht, dann steht sie.

Will man zu einem späteren Zeitpunkt eventuell Volumes vergrößern, sollte man auch das einmal durchspielen, bevor das System in den Produktiveinsatz geht. Dazu gehört aber nicht nur das Vergrößern des Volumes auf dem Disk-Subsystem, sondern auch das des Dateisystems [2]. Erst im letzten Schritt beginnt man mit dem Kopieren der Produktivdaten auf das neue System und den Lasttests mit der geplanten Anwendung.

Tauchen auf dem Weg zwischen dem Verkabeln und dem produktiven Einsatz größere Schwierigkeiten oder Phänomene auf, die man sich nicht erklären kann, sollte man nicht zu lange zögern, den Support zu kontaktieren. Etliche Stolpersteine sind den Herstellern, Systemhäusern und Distributoren bekannt und lassen sich schnell aus dem Weg räumen, zumal gerade die Hersteller seit Jahren große Kompatibilitätsdatenbanken pflegen. Deshalb sind auch neue Gerätekombinationen und ihr Verhalten für sie nicht uninteressant.

Vorsicht ist allerdings angeraten, wenn ein Hersteller versucht, die Schuld auf den nächsten abzuwälzen, etwa der HBA-Bauer auf den des Switches und so weiter. Aus dieser Endlosschleife kommt man meist nur heraus, wenn man darauf besteht, dass sie die Frage der Zuständigkeit untereinander klären. Erspart bleibt einem das, wenn man als Ansprechpartner ein Systemhaus oder einen Distributor hat, der die Komponenten, also Disksubsystem, Switch, HBAs und Betriebssystem in der gewünschten Kombination getestet hat oder vor der Auslieferung testet.

Fazit

Hat man sich erst einmal mit der FC-Technik auseinandergesetzt, ist der Aufbau eines SANs nicht schwieriger als der eines LANs. Die Tücken liegen vor allem bei den Anbieter-Versprechen („alles Plug & Play“) und in verkonfiguriert gelieferten Geräten. Doch selbst wenn das Aufbauen des Netzes ohne Schwierigkeiten vonstatten geht, beginnt dann erst die richtige Arbeit: das Einrichten der Volumes, das unumgängliche Zuordnen (Privatisieren) von Volumes und Servern, das Testen, das Kopieren der Daten und nicht zu vergessen das Trennen der Ethernet-basierten Management-Schnittstellen von den Netzsegmenten der Abteilungen und der Server. (sun)

Literatur

[1] Susanne Nolte; Lichtwellenleiter; Kleine Kabelage; Glasfaserkabel und Stecker im Griff; *iX* 1/2005, S. 128

[2] Michael Riepe; Tools und Tipps; Möbelpacker; Dateisysteme kopieren, vergrößern und verkleinern; *iX* 8/2008, S. 145

Troubleshooting-Tipps

1) read the fucking manual
2) Schritt für Schritt vorgehen
3) nach jedem Schritt Ergebnis prüfen
4) erst Port-zu-Port-Verbindungen prüfen, dann von Endpunkt zu Endpunkt
5) gegebenenfalls erst die Zonen, dann die Volumes einrichten
6) die frisch angelegten Volumes sofort den zugehörigen Servern zuweisen
7) vor dem Produktivbetrieb Performance, Stabilität und später benötigte Features wie Volume-Expandieren testen



Geodaten: Quellen und Zugriffsmöglichkeiten

Globales Design

Tiziana Margaria-Steffen, Eldar Sultanow

Große Mengen von Geodaten schlummern in den Untiefen des Web. Dazu zählen Dienste für Routenplanung, Wetterberichte sowie Satelliten- und Luftbildkataloge. Mit geeigneten Werkzeugen und Strategien lassen sich über Webservices die zahlreichen Lager für geografische Informationen anzapfen.

Bund und Länder, Kataster- und Landesvermessungsämter, Unternehmen, Geo-, Polar- und Meeresforschungsinstitute stellen Geodaten strukturiert über das Web (meist in Form von Webservices) zur Verfügung. Je nach Intention, Qualität und Detaillierungstiefe bekommt man sie entweder kostenfrei oder muss einen Obolus entrichten. Standardisierung ist dabei in zweierlei Hinsicht notwendig: Zum einen garantiert sie Herstellerunabhängigkeit, zum anderen bildet sie die Voraussetzung für das Zusammenwirken der Dienste. Dieser Artikel zeigt, wie man via Webservices an Geodaten herankommt und sie visualisiert. Alle hier beispielhaft genannten Quellen sind frei.

Um die notwendigen Standards kümmert sich das internationale, nicht profitorientierte Open Geospatial Consortium (OGC). Zu den hier erstellten Spezifikationen gehören die Geography Markup Language (GML) sowie die Dienste Web Map Service (WMS), Web Feature Service (WFS) und Web Coverage Service (WCS). Das Webservice-basierte Konzept der Organisation soll einen Umschwung bei der Entwicklung geografischer Informationssysteme (GIS) bewirken – weg von monolithischen Systemen hin zu verteilten Diensten.

GML: Karriere als ISO-Standard

Die Norm ISO 19139 legt ein XML Schema für geografische Metadatenelemente auf Basis von ISO 19115 fest. Über das Schema lassen sich Metadatensätze mit geogafischem Inhalt zwischen verschiedenen Systemen austauschen. Dafür sowie für das Beschreiben und Speichern von Geometrien inklusive der zugehörigen Attribute ist die GML zuständig, die derzeit die Versionsnummer 3.2.1. trägt und seit dieser Release selbst ISO-Standard (ISO 19136) ist. Voraussetzung dafür war die Zusammenführung der OGC-Spezifikation mit der ISO-Reihe 191xx. GML berücksichtigt vor allem die Raumbezugsgrundformen in ISO 19107. Als die GML im Jahre 2000 erstmalig vorgestellt wurde, war eine solche Karriere keinesfalls absehbar [1].

Für die Übernahme als ISO-Norm hat die OGC alle veralteten Schema-Elemente aus GML 2.1 (in Version 3.0 als „deprecated“ gekennzeichnet) entfernt. Beispielsweise wurde *gml:NULL* durch das Attribut *nillable* und *gml:coordinates* durch *gml:posList* ersetzt. Winkel werden nun als Dezimalzahl angegeben (anstelle Grad/Minuten/Sekunden), Richtungen in Vektorform (*gml:vector*) anstelle von Polarkoordinaten (*gml:horizontalAngle* und *gml:verticalAngle*). Das *gml:id*-Attribut ist zwingend vorge-

iX-TRACT

- Da Anwendungen mit geografischem Bezug sich allgemein großer Beliebtheit erfreuen, findet man inzwischen viele kommerzielle und freie Geodaten im Web.
- Mithilfe freier Werkzeuge sowie mit den von der OGC standardisierten Webservices lassen sich Geodaten komfortabel auf den Rechner laden.
- Als Beschreibungssprache für Geodaten fungiert die GML, die es aus ihrem anfänglichen Schattendasein heraus bis zum ISO-Standard gebracht hat.

Listing 1: Ergebnis *GetCapabilities*

```
...
<ows:Title>My GeoServer WFS</ows:Title>
<ows:Abstract>
    This is a description of your Web Feature Server.
    The GeoServer is a full transactional Web Feature Server,
    you may wish to limit GeoServer to a Basic service level to
    prevent modificaiton of your geographic data.
</ows:Abstract>
...
<FeatureType xmlns:topp="http://www.openplans.org/topp">
    <Name>topp:states</Name>
    <Title>USA Population</Title>
    <Abstract>This is some census data on the states.</Abstract>
    <ows:Keywords>
        <ows:Keyword>
            census state boundaries united states
        </ows:Keyword>
    </ows:Keywords>
    <DefaultSRS>urn:x-ogc:def:crs:EPSG:6.11.2:4326</DefaultSRS>
    <OutputFormats>
        <Format>GML2</Format>
        <Format>GML2-GZIP</Format>
        <Format>text/xml; subtype=gml/2.1.2</Format>
        <Format>text/xml; subtype=gml/3.1.1</Format>
        <Format>gml3</Format>
        <Format>json</Format>
        <Format>SHAPE-ZIP</Format>
    </OutputFormats>
    <ows:WGS84BoundingBox>
        <ows:LowerCorner>-124.731422 24.955967</ows:LowerCorner>
        <ows:UpperCorner>-66.969849 49.371735</ows:UpperCorner>
    </ows:WGS84BoundingBox>
</FeatureType>
...
```

Listing 2: XML-Anfrage an Geo-Server

```
<?xml version="1.0" encoding="utf-8"?>
<GetFeature
  xmlns="http://www.opengis.net/wfs"
  xmlns:topp="http://www.openplans.org/topp"
  xmlns:ogc="http://www.opengis.net/ogc"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
service="WFS"
  version="1.1.0" outputFormat="text/xml; subtype=gml/2.1.2"
  maxFeatures="100" handle="">
  <Query typeName="topp:states" srsName="EPSG:4326">
     <ogc:Filter>
       <ogc:Within>
      <ogc:PropertyName>topp:the_geom</ogc:PropertyName>
          <gml:Envelope srsName="EPSG:4326"
          xmlns:gml="http://www.opengis.net/gml">
          <gml:lowerCorner>
               -124.731422 18.9604888249186
          </gml:lowerCorner>
          <gml:upperCorner>
               -66.969849 55.3672131750814
          </gml:upperCorner>
          </gml:Envelope>
             </ogc:Within>
    </ogc:Filter>
  </Query>
</GetFeature>
```



Gaia stellt die aus dem Web geladenen verschiedenen Layer übereinander dar (Abb. 1).

Listing 3: Ergebnis XML-Anfrage

```
<?xml version="1.0" encoding="UTF-8"?>
<wfs:FeatureCollection numberOfFeatures="49"
    ...
    <gml:featureMembers>
      <topp:states gml:id="states.1">
      <gml:boundedBy>
        <gml:Envelope
           srsName="urn:x-ogc:def:crs:EPSG:6.11.2:4326">
              <gml:lowerCorner>
                  36.98677100000005 -91.516129
              </gml:lowerCorner>
              <gml:upperCorner>
                  42.50936100000001 -87.507889
              </gml:upperCorner>
          </gml:Envelope>
      </gml:boundedBy>
      <topp:the_geom>
          <gml:MultiSurface
           srsName="urn:x-ogc:def:crs:EPSG:6.11.2:4326">
            <gml:surfaceMember>
           <gml:Polygon> <gml:exterior>
              <gml:LinearRing> <gml:posList>
              37.51099000000001 -88.071564
              37.476273000000006 -88.087883
              37.442852 -88.311707
              37.40930899999999 -88.359177
              ...
              </gml:posList> </gml:LinearRing>
              </gml:exterior> </gml:Polygon>
            </gml:surfaceMember>
          </gml:MultiSurface>
     </topp:the_geom>
     <topp:STATE_NAME>Illinois</topp:STATE_NAME>
     <topp:STATE_ABBR>IL</topp:STATE_ABBR>
     ...
     <topp:LAND_KM>143986.61</topp:LAND_KM>
     <topp:WATER_KM>1993.335</topp:WATER_KM>
     <topp:PERSONS>1.1430602E7</topp:PERSONS>
     <topp:FAMILIES>2924880.0</topp:FAMILIES>
     <topp:HOUSHOLD>4202240.0</topp:HOUSHOLD>
     <topp:MALE>5552233.0</topp:MALE>
     <topp:FEMALE>5878369.0</topp:FEMALE>
     <topp:WORKERS>4199206.0</topp:WORKERS>
     ...
     <topp:EMPLOYED>5417967.0</topp:EMPLOYED>
     <topp:UNEMPLOY>385040.0</topp:UNEMPLOY>
     ...
     </topp:states>
     <topp:states gml:id="states.2">
     ...
     </topp:states>
 </gml:featureMembers>
</wfs:FeatureCollection>
```

schrieben (mandatory), XLink zum Referenzieren von GML-Objekten erlaubt. Und das XML Schema lässt sich jetzt von der XSD-Datei trennen.

Serviceorientierte Architekturen (SOA) gewinnen im Geobereich an Bedeutung. Die GML ermöglicht den Datenaustausch von Vektordaten zwischen verteilten Datenquellen und -diensten. Sie hat inzwischen einen beachtlichen Leistungsumfang, aber auch einen hohen Grad an Komplexität erreicht. GML-Profile (Subset der Spezifikation) bieten die Möglichkeit, die Markup Language in einem abgespeckten, anwendungsspezifischen Modus zu verwenden.

GML nutzt XML sowie die notwendigen Konstrukte, etwa Daten- und Geometrietypen einschließlich deren Kodierung. Die Metasprache legt Austauschformate für Geodaten fest. Sie gibt den Modellierungsrahmen vor und bietet eine große Auswahl an direkt einsetzbaren Geometrieelementen. Verschiedene Anwendungen haben jeweils eigene Schemata und Ausprägungen. Geografische Objekte (technisch Features genannt) können zum Beispiel Gebäude, Flüsse, Flurstücke, Lagefestpunkte, Eigentümer oder Nutzungsflächen sein. Eine Menge solcher Features ergeben Feature Collections, etwa Katasterauszüge.

Ab Version 3 unterstützt GML neben Geometrien wie Bögen, Bézierkurven und Splines die Kodierung von Topologien, 3D-Objekten, zeitlichen Abläufen, Punktmengenobjekten, die Erstellung von eigenen Referenzsystemen sowie Maßeinheiten und Datenqualitätsinformationen. Zu Validierungszwecken lassen sich entsprechende XML-Schema-Werkzeuge einsetzen. Im Zuge der Weiterentwicklung der GML hat auch die Anzahl der Schemata zugenommen. Zurzeit umfasst die Sprache mehr als dreißig Kernschemata, die sich zur Definition eines Anwendungsschemas einsetzen lassen.

Geodaten aus dem Web saugen

Im Folgenden werden die Dienste WFS und WCS näher vorgestellt. Letzterer befasst sich ausschließlich mit Rasterdaten, WFS beschränkt sich auf Vektordaten (siehe Kasten „Onlinequellen“ sowie *iX*-Link am Ende des Textes). WFS sind im Web zahlreich zu finden, erlauben den Zugriff auf geografische Objekte in Datenbanken und geben das Ergebnis im GML-Format zurück.

Eine Anfrage an einen WFS erfolgt als HTTP-Request. Jeder WFS beherrscht fünf Operationen. Via *GetCapabilties* ermittelt der Client seine Fähigkeiten sowie die angebotenen Feature Types (Kategorien). *DescribeFeatureType* enthüllt deren Struktur. Abschließend fordert der Client mit *GetFeature* eine Instanz eines Feature an (das kann beispielsweise ein konkreter Fluss sein). Bei einem WFS mit Schreibzugriff lässt sich die *Transaction*- (Anlegen, Ändern, Löschen) oder die *Lock-Feature*-Anfrage (Sperre auf einem

Feature) stellen. Als Beispiel soll hier der My Geoserver dienen. Die *GetCapability*-Anfrage sieht wie folgt aus:

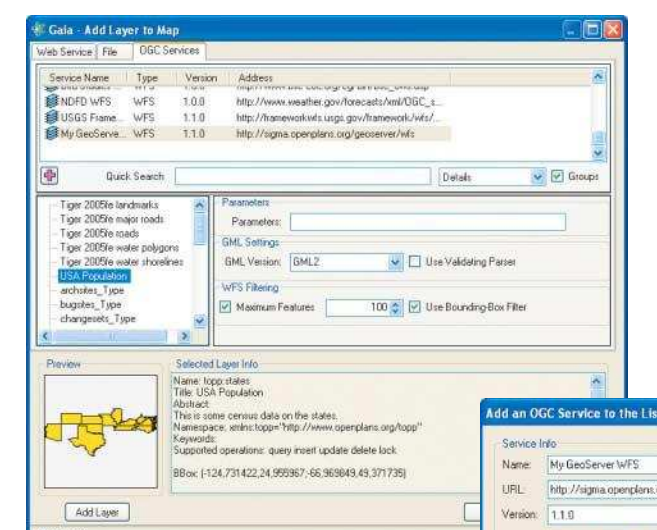
```
sigma.openplans.org/geoserver/wfs?request= ↵
GetCapabilities
```

Als Ergebnis erhält man den in Listing 1 ausschnittsweise dargestellten Code zurück (die vollständigen Listings liegen auf dem FTP-Server der *iX*). Es folgt die *GetFeature*-Anfrage nach *topp:states (USA Population)*:

```
sigma.openplans.org/geoserver/wfs?request= ↵
GetFeature&typeName=topp:states
```

In XML sieht diese Anfrage wie in Listing 2 aus. Daraufhin erhält man die entsprechenden Vektordaten (Listing 3). Die Antwort enthält Angaben zur Bevölkerung (männlich, weiblich, Familien, Arbeitnehmer et cetera). Abbildung 1 zeigt die für die Ausgabe aufbereiteten GML-Vektordaten (erstellt mit dem freien Tool Gaia). Es gibt etliche Programme und Klassenbibliotheken zum Visualisieren von GML-Daten, etwa GDAL (Geospatial Data Abstraction Library) und MapXtend, eine auf Java basierende API und Engine, die raumbezogene Daten und Inhalte für die Verwendung auf mobilen Endgeräten aufbereitet. Rendering von GML-Daten ist hier nur eine Funktion.

Tools –> Add Layer (Abbildung 1) führt zum Gaia-Dialog „Add layer to Map" (Abbildung 2, links). Über den Plus-Button wird ein neuer Eintrag angelegt, es erscheint die zuständige Maske „Add an OGC Service to the List" Abbildung 2, rechts). Hier muss man die notwendigen Angaben machen. Die Beschreibung lässt sich aus der Antwort der *GetCapabilities*-Anfrage übernehmen (Listing 1, oben). *Service Type* soll auf *WSF* stehen (WMS und WCS wären mit entsprechender URL grundsätzlich ebenfalls möglich). Dann wählt man aus der Feature-Liste *USA Population* aus und erhält eine Vorschau (Abbildung 2, links). Das Hinzufügen weiterer Layer ergibt schließlich die USA-Karte. Dieser Ablauf lässt sich mit beliebigen WFS durchführen.



In den Dialog links gibt man die Adresse eines beliebigen Webservice ein. Rechts lassen sich der angeforderten Karte Layer hinzufügen (Abb. 2).

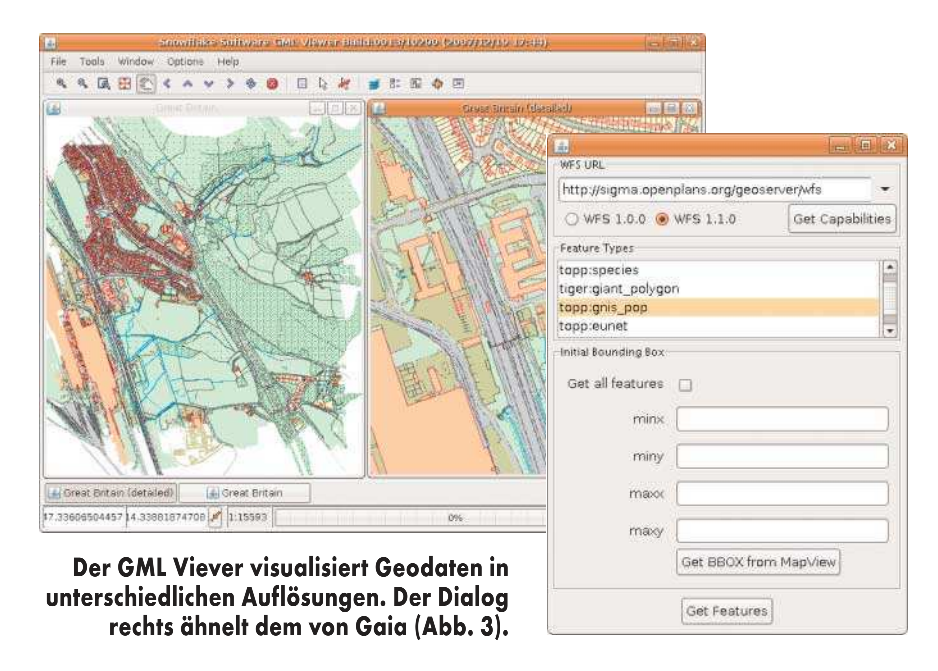
Geodaten richtig visualisiert

Ein ebenfalls geeignetes Werkzeug zum Visualisieren von GML-Daten ist der GML Viewer der Firma Snowflake. Er lässt sich entweder als Installationspaket für verschiedene Betriebssysteme oder als generisches Java-Archiv frei herunterladen. Auf seiner Webseite liegen detailreiche Beispieldaten im GML-2- und GML-3-Format zu den Niederlanden, Deutschland und Großbritannien. Letztere illustriert die Abbildung 3 in Kompakt- und Detailansicht. Auf Wunsch zeigt das Werkzeug beliebig viele Fenster zu einem Layer an.

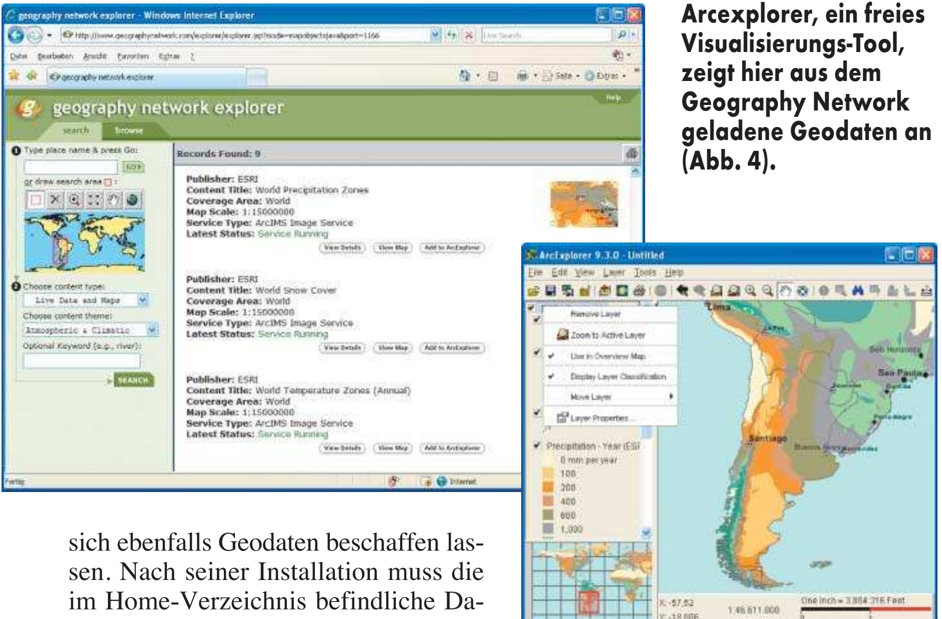
Über den Viewer lassen sich ebenfalls WFS-Daten laden. Dazu *File –> Open WFS (Beta)* öffnen. Es erscheint ein Dialog (Abbildung 3, rechts), in dem man die URL des WFS angibt. Ein Klick auf *Get Capabilities* listet seine Features. Zur Ermittlung der Bounding-Box-Koordinaten dient der Button *Get BBOX from MapView*.

WCS ist der OGC-Standard für den Zugriff auf Rasterdaten (Coverages). Als Rasterbilder bezeichnet man eine Art der geometrischen Anzeige von raumbezogenen Objekten in Matrixform (Zeilen und Spalten). Diese Datenstruktur nutzt in der Regel quadratische Zellen gleicher Größe. Die meisten Bilder in der GIS-Welt bestehen aus Rasterdaten. Es lassen sich damit jedoch auch beliebige andere numerische Informationen darstellen, etwa Messwerte. Die Hauptanwendungen von Rasterdaten liegen in der digitalen Photogrammetrie (Bildmessung, Bestimmung der räumlichen Lage, dreidimensionale Formen aus Fotografien), der Fernerkundung und der thematischen Kartografie. In der Datenanalyse zeigen Rasterdaten ebenfalls ihre Vorzüge, ebenso wie beim Aufbau digitaler Geländemodelle.

Esri ist der führende Hersteller im Bereich von GIS-Basissoftware. Neben seinen kommerziellen Tools stellt das Unternehmen den kostenfreien Viewer Arcexplorer zur Verfügung, mit dem



Der GML Viever visualisiert Geodaten in unterschiedlichen Auflösungen. Der Dialog rechts ähnelt dem von Gaia (Abb. 3).



Arcexplorer, ein freies Visualisierungs-Tool, zeigt hier aus dem Geography Network geladene Geodaten an (Abb. 4).

sich ebenfalls Geodaten beschaffen lassen. Nach seiner Installation muss die im Home-Verzeichnis befindliche Datei *aimsclient.properties* folgendermaßen angepasst werden:

```
WebBrowser=C\:/Programme/Internet
Explorer/iexplore.exe
WebBrowser.usesQuotes=false
AEJavaHelp=C\:/Programme/ArcGIS/ ↵
                    ArcExplorer/Help/aejava_help.htm
```

Dann startet man den Viewer und wählt *Layer -> Geography Network*. Es öffnet sich (in diesem Fall) der Internet Explorer mit der Website des Geography Network Explorer. Abbildung 4 zeigt links eine Weltkarte, in der man mit der Maus einen gewünschten Ausschnitt wählt (hier Südamerika, Westen, Bereich Chile). Als zweites einschränkendes Kriterium kommt hier Atmospheric & Climatic zum Zuge. Es gibt eine ganze Palette weiterer Möglichkeiten (Binnengewässer, Kultur und Demografie, Biologie und Ökologie et cetera).

Karten mit zahlreichen Funktionen

Ein Klick auf *Search* listet die gefundenen Geodaten auf. Aus diesen sucht man sich Ergebnisse aus (*Add to ArcExplorer*). Wer im ersten Suchergebnis „World Precipitation Zones“ (weltweite Niederschlagszonen) auswählt, bekommt die entsprechende Karte (Abbildung 4, rechts). Hier kann man zoomen, neue Layer hinzufügen, umsortieren et cetera.

Als industrielles Anwendungsbeispiel soll hier der europäische Programmierwettbewerb von Ricoh Europe und Kosponsor Sun dienen. Aufgabe war es, Java-Anwendungen zu entwickeln, die sich auf Ricohs Aficio-Laserdruckern und Multifunktionssystemen einsetzen lassen. Das von Benjamin Hanzelmann und Stefan Naujokat mit jABC [2] entwickelte System erreichte das nationale Finale [3]. Die Applikation besteht aus Internet- und Druckerdiensten sowie eigenen Routinen. Das im Drucker eingebettete System scannt Visitenkarten und extrahiert die Postleitzahl via OCR (Optical Character Recognition). Von der Postleitzahl ausgehend wird die geografische Umgebungskarte generiert. Dabei helfen drei Webservices der PRO DV aus Dortmund. Der erste ermittelt aus einer Adresse (Postleitzahl und Stadt) eine Koordinate. Wer es genauer haben will, gibt zusätzlich Straße und Hausnummer an. Bei dieser Geocodierung kommen Daten der Firma Tele Atlas zum Einsatz:

```
<<PRO_DV_GeoServer>/GeocoderServlet?PLZ= ↵
44227&ORT=Dortmund&STRASSE=Kohlenbankweg
```

Der zweite Service berechnet den Kartenausschnitt anhand der Koordinate, die den Mittelpunkt bildet. Zusätzlich kann man Informationen zur Ausdehnung der Karte in West-Ost- und in Nord-Süd-Richtung in Meter übergeben (Bounding Box):

```
<<PRO_DV_GeoServer>/BoundingBoxServlet?x= ↵
7.407990&y=51.482125&width=500&height=500
```

Mit diesen Informationen lässt sich der dritte Service, ein WMS, abfragen, (hier auf Basis des Produkts Mapxtreme von Mapinfo). Beispielsweise übergibt der Entwickler das Bildformat, die Hintergrundfarbe und die Bounding-Box-Koordinaten (*format=image/gif*, *bgcolor=0xffffff*, *bbox=7.451763,51.516154,7.471763,51.5161543*). Der WMS liefert die Karte als Rasterbild zurück, das die Anwendung abschließend in PDF konvertiert. Die gewünschte Skalierung stellt der Benutzer direkt am Drucker ein. (jd)

PROF. DR.-ING. TIZIANA MARGARIA-STEFFEN

ist Inhaberin des Lehrstuhls für Service and Software Engineering an der Universität Potsdam.

ELDAR SULTANOW

arbeitet als J2EE-Entwickler/Architekt bei der Producto AG in Berlin.

Onlinequellen

Open Geospatial Consortium	www.opengeospatial.org
Web Feature Service Implementation	www.opengeospatial.org/standards/wfs
Web Map Server Implementation	www.opengeospatial.org/standards/wms
Web Coverage Service Implementation	www.opengeospatial.org/standards/wcs
Geography Markup Language	www.opengeospatial.org/standards/gml

Literatur

[1] Christian Wilk; Geodaten; Komplexe Nische; GML: geografischer Markup-Standard; *iX* 12/2006, S. 66

[2] Jane Fröming, Norbert Gronau, Eldar Sultanow; MDA-Werkzeuge; Softwareautomaten; Im Vergleich: jABC; AndroMDA und OpenArchitectureWare; *iX* 8/2008, S. 92

[3] Benjamin Hanzelmann, Stefan Naujokat; Embedded System Workflow Execution with jABC and jAWS; Chair of Programming Systems, University of Dortmund, 2007

iX-Link ix0809139





Silverlight-2-Tutorial, Teil II: Digitales Fotoalbum

Bildwechsel

Regina Dowling, Jörg Müller

Zu den beliebten Webanwendungen gehört ein digitales Fotoalbum. Mit einigen Standard-Controls aus dem Silverlight-Paket und einem in Expression Blend entworfenen Layout lässt sich eine Webseite mit Thumbnails und Detailansichten relativ schnell realisieren.

Nachdem der erste Teil des Tutorials einen Überblick über die Fähigkeiten von Silverlight 2 gegeben hat, kommen im zweiten einige davon zur Anwendung. Als praxisnahe Beispielapplikation soll dazu ein einfaches Fotoalbum entstehen, das eine Reihe von JPG-Dateien von einem Webserver als Thumbnails und auf Klick als Detailansicht anzeigt. Für das Layout der Anwendung und die Gestaltung des Hintergrunds wird Expression Blend eingesetzt.

Neben einigen Standard-Controls, die im Silverlight-Paket schon enthalten sind (*Grid, ScrollViewer, StackPanel* und *Image*) nutzt die Anwendung ein benutzerdefiniertes Steuerelement.

Außerdem zeigt dieser zweite Teil die Verarbeitung von Maus-Ereignissen, das Erzeugen und Manipulieren von Control-Instanzen via Code sowie die Definition von Animationen per XAML.

Vorzüge durch zwei Werkzeuge

Wie aus Teil I bereits bekannt, kann man ein neues Silverlight-Projekt entweder im Visual Studio oder in Expression Blend anlegen. Wählt man das Visual Studio, hat man den Vorteil, dass die IDE zu jedem XAML-Objekt die Code-behind-Datei gleich mit anlegt.

Unabhängig von der gewählten Startumgebung lassen sich die XAML-Dateien sowohl in Visual Studio als auch in Expression Blend bearbeiten. Grafische Elemente sind oft einfacher in Blend zu erstellen und zu ändern, während Visual Studio die Arbeit im XAML-Code durch die Intellisense-Unterstützung erheblich vereinfacht. So kann der Entwickler die Vorzüge beider Werkzeuge nutzen.

Über das Kontextmenü der XAML-Dateien kann er problemlos und jederzeit zwischen beiden Umgebungen wechseln. Dabei darf das Projekt in beiden Anwendungen geöffnet sein; bei Bedarf werden offene Änderungen beim Wechsel gespeichert und das jeweils andere Programm lädt das Projekt automatisch neu.

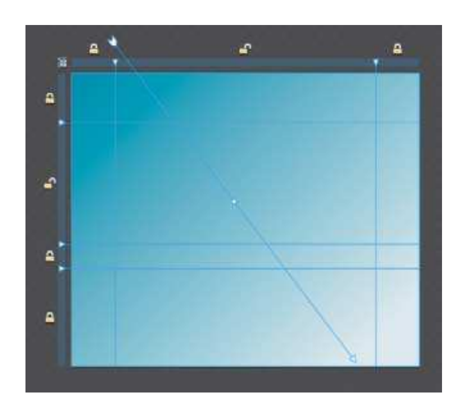
Beim Anlegen des Projekts *FotoAlbum* sollte man nicht nur eine statische Testseite, sondern gleichzeitig eine passende Webseite erstellen. Die aus dem Web geladenen Bilder können nur angezeigt werden, wenn der Aufruf der Anwendung über einen Webserver erfolgt.

Die *Page*, das Haupt-XAML-Dokument einer Silverlight-2-Anwendung, ist bereits ein eigenes *User*-Control. Innerhalb der *Page* kann man in einem *Grid* namens *LayoutRoot* bestimmen, wie die Anwendung aussieht (Listing 1).

Layout-Definition mit Farbverlauf

Beim *FotoAlbum* soll es einen Farbverlauf im Hintergrund geben. Diesen Verlauf kann *LayoutRoot* als Hintergrund definieren, und über das Properties-Panel in Blend lässt er sich einstellen. Das „Brush Transform“-Werkzeug kann das Aussehen des Verlaufs (Richtung, Start- und Endpunkt) nach Wunsch verändern (Abbildung 1).

Zur Aufteilung des Bildschirms legt der Entwickler Zeilen und Spalten im *Grid* fest und zwar mithilfe der Property *Grid.RowDefinitions* beziehungsweise *Grid.ColumnDefinitions*. Das *FotoAlbum* soll aus zwei Hauptbereichen bestehen: einer Leiste mit Thumbnails der verfügbaren Bilder sowie der Detailansicht des ausgewählten Bilds. Also muss auch das *LayoutRoot*-Grid in entsprechende Zeilen und Spalten unterteilt werden, was entweder im Design-



Den Farbverlauf des Hintergrunds kann der Entwickler mithilfe des „Brush Transform“-Werkzeugs anpassen (Abb. 1).

Listing 1: Layout der Anwendung

```
<UserControl x:Class="FotoAlbum.Page"
xmlns="http://schemas.microsoft.com/winfx/2006/xaml/pre-
sentation"
xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
Width="Auto"
Height="Auto">
   <Grid x:Name="LayoutRoot" >
      <Grid.Background>
         <LinearGradientBrush EndPoint="0.8, 0.9"
                              StartPoint="0.1,-0.09">
            <GradientStop Color="#FF7CA5BF"/>
            <GradientStop Color="#FFE0E7EC" Offset="1"/>
         </LinearGradientBrush>
      </Grid.Background>
      <Grid.RowDefinitions>
         <RowDefinition Height="80"/>
         <RowDefinition Height="*"/>
         <RowDefinition Height="40"/>
         <RowDefinition Height="160"/>
      </Grid.RowDefinitions>
      <Grid.ColumnDefinitions>
         <ColumnDefinition Width="80"/>
         <ColumnDefinition Width="*"/>
         <ColumnDefinition Width="80"/>
      </Grid.ColumnDefinitions>
      <!-- ... -->
   </Grid>
</UserControl>
```

Listing 2: Platzhalter für die Detailansicht

```
...
 <Image x:Name="DetailView" Grid.Column="1" Grid.Row="1"
Source="" >
    <Image.Resources>
       <Storyboard x:Name="FadeInAnimation">
          <DoubleAnimation Duration="00:00:00.40" From="0"
To="1"
             Storyboard.TargetProperty="Opacity"
             Storyboard.TargetName="DetailView" />
       </Storyboard¬ª
       <Storyboard x:Name="FadeOutAnimation">
          <DoubleAnimation Duration="00:00:00.40" From="1"
To="0"
             Storyboard.TargetProperty="Opacity"
             Storyboard.TargetName="DetailView" />
       </Storyboard>
    </Image.Resources>
 </Image>
...
```

Im Design-View von Expression Blend kann der Entwickler über das *LayoutRoot*-Grid den Bildschirm in Zeilen und Spalten einteilen (Abb. 2).

View oder direkt im XAML-Code möglich ist. Dabei kann die Angabe der einzelnen Zeilen- und Spaltengrößen relativ oder absolut sein, man kann aber auch eine automatische Größenanpassung (*Auto*) wählen.

Die Detailansicht des ausgewählten Bildes, ein *Image*-Control namens *DetailView*, wird ebenfalls direkt innerhalb von *LayoutRoot* platziert (Listing 2). Dabei bestimmen die Properties *Grid.Row* und *Grid.Column* die Positionierung, die Indizes für Zeilen und Spalten des Grid starten bei 0. Das jeweils ausgewählte Bild soll in der mittleren Spalte und in der zweiten Zeile des Grid erscheinen.

Um das Bild ein- und ausblenden zu können, definiert der Entwickler innerhalb von *DetailView* zwei *Storyboards*, mit deren Hilfe er die Transparenz (die Eigenschaft *Opacity*) des Bildes animieren kann. Die *Storyboards* legt er als Ressourcen an, über eine eindeutige ID kann er sie per Code ansprechen. Jedes *Storyboard* enthält ein Animationselement vom Typ *DoubleAnimation* (d. h. der animierte Wert ist vom Typ *Double*).

Ein Animationsobjekt kann genau eine Eigenschaft (*Storyboard.TargetProperty*) eines Elements (*Storyboard.TargetName*) verändern. Die Parameter *From* und *To* legen fest, welcher Wert am Anfang und welcher am Ende der Animation erreicht werden soll, die *Duration* gibt die Dauer der Animation an.

Bildauswahl über eigene Leiste

Da beim Start der Anwendung noch kein Bild ausgewählt wurde, wird keine *Source* für das *Image*-Objekt angegeben, die Eigenschaft wird erst später, beim Klick auf eins der Thumbnail-Bilder gesetzt. Dazu unten mehr.

Neben dem *Image*-Control für die Detail-Ansicht enthält das *LayoutRoot*-Grid ein *ScrollViewer*-Control, das als Container für die Liste der verfügbaren Thumbnails dient (Listing 3). Auf diese Weise kann der Anwender die Thumbnail-Leiste bei Bedarf bequem scrollen. Dabei ist der Scroll-Balken nur sichtbar, wenn er tatsächlich benötigt wird, zum Beispiel, wenn eine größere Anzahl an Thumbnails sichtbar sein oder die Größe des Browserfensters geändert werden soll.

Damit man keinen Übergang zwischen dem *ScrollViewer* und dem Rest der Anwendung sieht, wird der Rahmen des *ScrollViewer* über die Eigenschaft *BorderThickness* unsichtbar gemacht. Die Bilderleiste bekommt ihren Platz in der zweituntersten Zeile von *LayoutRoot* und umfasst alle drei Spalten, das heißt im Gegensatz zur Detailansicht braucht die Bilderleiste keinen horizontalen Abstand zum Rand der Anwendung.

Um die Anordnung der einzelnen Thumbnails zu erleichtern, enthält der *ScrollViewer* ein *StackPanel*-Control, das seine Inhalte automatisch horizon-

iX-TRACT

- Als Silverlight-Beispielanwendung für das Tutorial dient ein digitales Fotoalbum, das zum Teil in Visual Studio und zum Teil in Expression Blend entwickelt wird.
- Das Projekt kann parallel in beiden Entwicklungsumgebungen geöffnet sein; ein Wechsel ist über das Kontextmenü der XAML-Dateien jederzeit möglich, wobei sichergestellt bleibt, dass beide Versionen auf dem aktuellen Stand sind.
- Das Erscheinungsbild der Anwendung definieren im Wesentlichen zwei XAML-Dateien, die über Code-behind-Klassen miteinander verknüpft werden. Sollen später noch Oberflächenelemente hinzugefügt werden, kann der Entwickler den Sourcecode entsprechend ergänzen.

Controls dynamisch erzeugen

In Silverlight 2 sind alle XAML-Controls isomorph mit CLR-Objekten, das heißt, alle Objekte, die sich mit XAML definieren lassen, kann man genauso gut per Code generieren. Ein in XAML per

```
<Button x:Name="myButton" Content="Hallo" />
```

deklarierter Button lässt sich äquivalent mit folgenden Codezeilen erzeugen:

```
Button myButton = new Button();
myButton.Content = "Hallo";
```

Obwohl es möglich ist, alle Elemente per Code zu erzeugen, gilt es als „best practice“, die Elemente in der Regel per XAML zu definieren, da die Anwendung im Bedarfsfall auf diese Weise einfacher zu modifizieren, zu skalieren und zu warten ist.

Andererseits gibt es immer wieder Projekte, bei denen man zum Zeitpunkt der Entwicklung nicht genau vorhersagen kann, welche und wie viele Elemente die Anwendung zur Laufzeit tatsächlich benötigt. In solchen Fällen ist es äußerst praktisch, dass man diese Elemente per Code „nachreichen“ kann.

Dabei darf man allerdings nicht vergessen, die betreffenden Elemente zum *LayoutRoot* oder einem anderen sichtbaren Element hinzuzufügen, damit sie tatsächlich in der Anwendung erscheinen.

Listing 3: Layout der Bildauswahl-Leiste

```
<ScrollViewer BorderThickness="0" Grid.Row="3" Grid.Column="0" Grid.ColumnSpan="3" HorizontalScrollBarVisibility="Auto"
                                                                        VerticalScrollBarVisibility="Hidden">
  <StackPanel x:Name="ThumbnailContainer" HorizontalAlignment="Center" VerticalAlignment="Stretch"
                                                                  Orientation="Horizontal" />
</ScrollViewer>
```

tal nebeneinander platziert. Da die Anzahl sowie die Sources der einzelnen Bilder flexibel sein sollen, wird im XAML nur das *StackPanel* angelegt, die Thumbnails selbst werden später in der Code-behind-Datei hinzugefügt. Eine eindeutige ID (*ThumbnailContainer*) sorgt dafür, dass man das *StackPanel* via Code ansprechen kann.

Da die Beispielanwendung die Thumbnail-Bilder mit Interaktionen und Animationen versehen soll, werden die gewünschten Funktionen zusammen mit dem betreffenden *Image*-Objekt in ein eigenes (benutzerdefiniertes) *User*-Control verpackt. Dazu wählt man im Kontext-Menü von Visual Studio (rechter Mausklick) des Projekts *FotoAlbum*: „Add“ > „New Item…“ > „Visual C#“ > „Silverlight User Control“ und gibt dem neuen Control den Namen *Thumbnail.xaml*.

Wie die *Page* ist das *Thumbnail*-Control von *UserControl* abgeleitet, entsprechend wird das Aussehen des Control innerhalb des *Grid LayoutRoot* definiert (Listing 4). *Thumbnail* enthält als einziges sichtbares Element ein *Image*-Objekt. Neben der ID (*ThumbnailImage*) definiert der Entwickler per XAML eine Reihe von Eigenschaften, die das Äußere des *Thumbnail* bestimmen, beispielsweise eine fixe Höhe sowie eine variable Breite (d. h. nicht alle Thumbnails müssen das gleiche Seitenformat haben) und so weiter. Die *Source* gibt der Entwickler später im Quellcode an.

Wenn der Benutzer mit der Maus über die Bilder in der Auswahlleiste fährt, soll die Anwendung sie vergrößert darstellen, außerdem soll die Detailansicht des Bildes erscheinen, sobald er mit der Maus auf das *Thumbnail* klickt. Daher müssen die Bilder auf drei verschiedene Maus-Ereignisse reagieren: *MouseEnter, MouseLeave* und *MouseLeftButtonDown*. Jedes der drei Ereignisse ruft einen eigenen Code-behind-Handler auf.

Hinter den Kulissen: Code-behind-Klassen

Die *Storyboard*s zum Vergrößern und Verkleinern des *Thumbnail* werden – wie zuvor die *Storyboards* der Detailansicht – als Ressourcen mit einer eindeutigen ID angelegt, weil ihr Aufruf aus dem Code heraus erfolgt. Was am Ende der Animation passiert, legt die Eigenschaft *FillBehaviour* fest. Der Wert *HoldEnd* besagt, dass die am Ende erreichten Werte bis zum Start eines neuen *Storyboard* beibehalten werden. Da jede *DoubleAnimation* immer nur eine Eigenschaft eines Objekts verändern kann, enthält jedes *Storyboard* zwei Animationselemente: Eine Animation ändert die Breite, die andere die Höhe des Bildes.

Debugging

Das Add-on von Visual Studio stellt einen Debugger für Silverlight-Projekte zur Verfügung, der sich nahtlos in die übliche Unterstützung bei der Fehlersuche integriert. Ein paar Punkte muss man beachten, auf die häufigsten Stolpersteine sei an dieser Stelle hingewiesen:

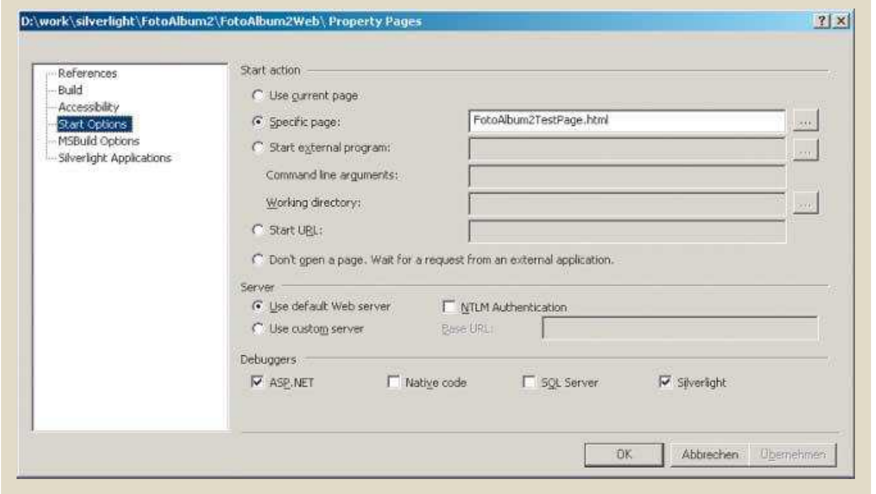
– Das Debugging erfolgt über das zu Beginn mit angelegte Webprojekt: In *web.config* muss daher generell *debug = true* gesetzt sein. Der Test erfolgt über den VS-internen Webserver. Steht der Wert nicht auf *true*, macht sich VS mit einer Fehlermeldung bemerkbar. Über die Auswahl eines Radiobutton kann der Anwender diese Einstellung direkt im Fehlerdialog ändern.

– In den Eigenschaften des Webprojekts („Start Options“ „Debugger“) muss zudem das Debugging für Silverlight-Projekte explizit erlaubt sein.

Danach kann man wie gewohnt beispielsweise Breakpoints setzen und das Debugging starten (über Menü „Debug“ > „Start Debugging“ oder F5).

Fehler bei der Fehlersuche

Wenn das Debugging trotzdem nicht funktionieren will: Die Betaversion der Silverlight Tools scheint sich in diesem Bereich nicht immer ganz fehlerfrei zu verhalten, wie zahlreiche Foren-Beiträge zum Thema beweisen. Im Zweifel lohnt sich immer ein Besuch der Silverlight-Community-Website (http://silverlight.net/forums/).



Über das Fenster „Property Pages“ kann der Entwickler den Silverlight-Debugger in Visual Studio starten (Abb. 3).

Das Aussehen der Anwendung definiert der Entwickler zwar hauptsächlich in den beiden XAML-Dateien für *Page* und *Thumbnail*, aber die einzelnen Elemente sind nicht automatisch miteinander verknüpft. Dies geschieht in den Code-behind-Klassen.

Beim Start verknüpft die Applikation im Konstruktor der *Page* das *Completed*-Event des *Storyboard* zum allmählichen Ausblenden der Detailansicht mit dem passenden Eventhandler *FadeOutAnim_Completed* (Listing 5). Dessen Aufruf erfolgt, wenn die Animation zum Ausblenden komplett abgelaufen ist. Der globalen Variablen *_sender* entnimmt die Anwendung dann das zuletzt angeklickte *Thumbnail*-Objekt, und erzeugt aus dessen Variable *imgSource* (über den Umweg über ein *Uri*-Objekt) ein neues *BitmapImage*. Dieses weist sie wiederum der Detailansicht als Quelle zu. Zuletzt startet das *Storyboard* zum Einblenden der Detailansicht.

Ebenfalls im Konstruktor erfolgt der Aufruf der Methode *InitThumbnails*, die die einzelnen Thumbnails erstellt. *InitThumbnails* ruft für jedes in der Auswahl angezeigte Bild die Methode *CreateThumbnail* auf und übergibt dieser den Pfad zur gewünschten Datei (in diesem Fall die absolute URL zu einem Bild auf einem Webserver, im Beispiel Flickr). Jeder Aufruf von *CreateThumbnail* erzeugt eine neue Instanz des *Thumbnail*-Control, deren benutzerdefiniertes Ereignis *ImageSelected* mit dem passenden Handler der *Page* (*Thumbnail_ImageSelected*) verknüpft wird. Anschließend wird die neue *Thumbnail*-Instanz dem *StackPanel ThumbnailContainer* hinzugefügt.

Tutorialinhalt

Teil I: Überblick Silverlight 2, Installation, Projektstruktur, erste Beispiel-Anwendung inklusive Button und Event-Handler

Teil II: Verwendung von Standard-Controls, Interaktivität, Drag & Drop, **Debugging, Einsatz von Expression Blend**

Teil III: Anbindung externer Daten, Deployment auf Silverlight Streaming

Wird eine neue Instanz des *Thumbnail*-Control erzeugt, bekommt der (überladene) Konstruktor der Klasse die URL des gewünschten Bildes als Parameter übergeben. Diesen Pfad speichert die Anwendung als String in der Property *imageSource*, eine Eigenschaft, die mithilfe der in VS 2008 eingeführten Syntax zur Initialisierung von Properties implementiert wird.

Bevor aus der Pfadangabe eine brauchbare *Source* für ein *Image*-Objekt werden kann, muss das Programm aus dem Pfad zunächst ein gültiges *Uri*-Objekt erzeugen, dieses dient wiederum als Input für ein neues *BitmapImage*-Objekt. Erst das *BitmapImage* kann man dem sichtbaren *Image*-Objekt als *Source* zuweisen (Listing 6). Diese umständliche Vorgehensweise ist erst seit Beta 2 erforderlich, in früheren Versionen konnte der Programmierer einen Pfad (String) direkt als *Source* angeben. Außerdem enthält die *Thumbnail*-Klasse die drei (bereits im XAML angekündigten) Eventhandler für die Mausereignisse, die es zu verarbeiten gilt: *ThumbnailImage_MouseEnter*, *ThumbnailImage_MouseLeave* sowie *ThumbnailImage_MousLeftButtonDown*.

Die beiden Handler *ThumbnailImage_MouseEnter* und *ThumbnailImage_MouseLeave* starten jeweils eins der *Storyboard*s zum Vergrößern beziehungsweise Verkleinern des Thumbnail-Bildes. Da jede Instanz des *Thumbnail*-Control über eigene *Storyboards* verfügt, können diese Animationen auch parallel zueinander laufen. Dies ist beispielsweise einer der Gründe, warum die Thumbnails nicht als normale *Image*-Controls implementiert wurden.

Außerdem wird für die Klasse *Thumbnail* ein eigener Event *ImageSelected* definiert. Dieses Ereignis erzeugt der dritte Maus-Handler beim Klick auf das Bild, und es enthält als Parameter eine Referenz auf das jeweilige Thumbnail sowie eine leere Instanz von *EventArgs* (im Beispiel benötigt der Handler keine weiteren Argumente).

Listing 4: XAML für das *Thumbnail*-Control

```
<UserControl x:Class="FotoAlbum.Thumbnail"
  xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
  xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml" ª
  <Grid x:Name="LayoutRoot">
     <Grid.Resources>
        <Storyboard x:Name="ZoomInAnim" FillBehavior="HoldEnd">
           <DoubleAnimation x:Name="ZoomInAnimW"
               Storyboard.TargetProperty="Width"
               Storyboard.TargetName="ThumbnailImage"
               To="140"
               Duration="00:00:00.2"/ª
           <DoubleAnimation x:Name="ZoomInAnimH"
               Storyboard.TargetProperty="Height"
               Storyboard.TargetName="ThumbnailImage"
               To="100"
               Duration="00:00:00.2"/>
        </Storyboard>
        <Storyboard x:Name="ZoomOutAnim" FillBehavior="HoldEnd">
           <DoubleAnimation x:Name="ZoomOutAnimW"
               Storyboard.TargetProperty="Width"
               Storyboard.TargetName="ThumbnailImage"
               To="79"
               Duration="00:00:00.2"/ª
           <DoubleAnimation x:Name="ZoomOutAnimH"
               Storyboard.TargetProperty="Height"
               Storyboard.TargetName="ThumbnailImage"
               To="55"
               Duration="00:00:00.2"/>
        </Storyboard>
     </Grid.Resources>
     <Image x:Name="ThumbnailImage"
        Width="Auto"
        Height="55"
        Stretch="Fill"
        Margin="5"
        Source=""
        MouseEnter="ThumbnailImage_MouseEnter"
        MouseLeave="ThumbnailImage_MouseLeave"
        MouseLeftButtonDown="ThumbnailImage_MouseLeftButtonDown" />
  </Grid>
</UserControl>
```

Listing 5: Die Klasse *Page.xaml.cs*

```
using System;
using System.Windows.Controls;
using System.Windows.Media;
using System.Windows.Media.Animation;
using System.Windows.Media.Imaging;
namespace FotoAlbum
{
    public partial class Page : UserControl
    {
        public Thumbnail _sender;
        public Page()
        {
            InitializeComponent();
            Storyboard FadeOutAnim = (Storyboard)this.FindName("FadeOutAnimation");
            FadeOutAnim.Completed += new EventHandler(FadeOutAnim_Completed);
            InitThumbnails();
        }
        private void CreateThumbnail(String img)
        {
            Thumbnail t = new Thumbnail(img);
            t.ImageSelected += new EventHandler(Thumbnail_ImageSelected);
            ThumbnailContainer.Children.Add(t);
        }
        private void InitThumbnails()
        {
            CreateThumbnail("http://farm2.static.flickr.com/1328/1422859939_b78ecb1196_o.jpg");
            CreateThumbnail("http://farm2.static.flickr.com/1180/1422928923_3c950be658_o.jpg");
            CreateThumbnail("http://farm2.static.flickr.com/1102/1423036119_ee2237203b_o.jpg");
            CreateThumbnail("http://farm2.static.flickr.com/1333/1423021817_da7f60150a_o.jpg");
             // ...
        }
        private void Thumbnail_ImageSelected(object sender, EventArgs e)
        {
            Storyboard FadeOutAnim = (Storyboard)this.FindName("FadeOutAnimation");
            _sender = (Thumbnail)sender;
            FadeOutAnim.Begin();
        }
        private void FadeOutAnim_Completed(object sender, EventArgs e)
        {
            Storyboard FadeInAnim = (Storyboard)this.FindName("FadeInAnimation");
            Uri uri = new Uri(_sender.imageSource, UriKind.RelativeOrAbsolute);
            BitmapImage img = new System.Windows.Media.Imaging.BitmapImage(uri);
            DetailView.SetValue(Image.SourceProperty, img);
            FadeInAnim.Begin();
        }
    }
}
```

Listing 6: Die Klasse *Thumbnail.xaml.cs*

```
using System;
using System.Windows.Controls;
using System.Windows.Media.Imaging;
using System.Windows.Input;
namespace FotoAlbum
{
    public partial class Thumbnail : UserControl
    {
        public event EventHandler ImageSelected;
        public Thumbnail()
        {
            InitializeComponent();
        }
        public String imageSource { get; set; }
        public Thumbnail(string imgSource)
        {
            InitializeComponent();
            imageSource = imgSource;
            Uri uri = new Uri(imgSource, UriKind.RelativeOrAbsolute);
            BitmapImage img = new System.Windows.Media.Imaging.BitmapImage(uri);
            ThumbnailImage.SetValue(Image.SourceProperty, img);
        }
        private void ThumbnailImage_MouseEnter(object sender, MouseEventArgs e)
        {
            ZoomInAnim.Begin();
        }
        private void ThumbnailImage_MouseLeave(object sender, MouseEventArgs e)
        {
            ZoomOutAnim.Begin();
        }
        private void ThumbnailImage_MouseLeftButtonDown(object sender, MouseButtonEventArgs e)
        {
            ImageSelected(this, this.EventArgs.Empty);
        }
    }
}
```

Klickt der Benutzer auf eines der Thumbnails, triggert das Ereignis *MouseLeftButtonDown* den Aufruf des Handler *ThumbnailImage_MouseLeftButtonDown*. Dieser erzeugt das benutzerdefinierte Ereignis *ImageSelected* und übergibt dabei eine Referenz auf das angeklickte Bild.

Den Event *ImageSelected* verarbeitet ein Handler in *Page.xaml.cs*. Darin wird die Methode *Thumbnail_ImageSelected* aufgerufen, die in einer globalen Variable speichert, welches *Thumbnail*-Objekt das Ereignis ausgelöst hat, und die anschließend das *Storyboard* zum Ausblenden der Detailansicht startet.

Das für diesen Tutorialteil angekündigte Thema Drag & Drop kommt hier nicht mehr zur Sprache, entfällt allerdings nicht, sondern wird Teil der dritten Folge sein, in der das Fotoalbum noch etwas ausgefeilter werden soll. Der Sourcecode für das vorgestellte Beispiel ist wie üblich über den *iX*-Listingservice erhältlich. (ka)

REGINA DOWLING

arbeitet als Multimedia-Programmiererin bei Berger Baader Hermes in München.

JÖRG MÜLLER

arbeitet als Head of Technology bei der Business Live GmbH in München.





Systemaktivität überwachen

Was los ist

Michael Riepe

Werden die Systemressourcen knapp, muss der Administrator eingreifen und sie aufstocken oder umverteilen. Der System Activity Reporter *sar* hilft bei der Bedarfsanalyse.

Antworten Server und Datenbank nicht schnell genug oder stürzen Anwendungen gar wegen Ressourcenmangels ab, muss der Admin handeln. Im Hinblick auf den Stromverbrauch sollte er das auch im umgekehrten Fall tun: wenn Server weitgehend ungenutzt herumstehen.

Dazu muss er zunächst feststellen, wie hoch die Auslastung seiner Systeme ist und welche Ressourcen wann und wie genutzt werden. Zur Debatte stehen nicht nur Rechenleistung und Speicherbedarf, sondern auch die Nutzung der Ein- und Ausgabekanäle zum Netz oder Massenspeicher sowie der Ressourcen des Betriebssystems – etwa Dateien, Prozesse oder Threads. Unix und seine Derivate bieten dafür eine Reihe von Werkzeugen, darunter den System Activity Reporter *sar* – unter Linux versteckt er sich im Paket *sysstat* (siehe Kasten „Onlinequellen“).

Alle Vorgänge im Blick

Mit dem Kommando *sar 10* kann sich der Nutzer alle zehn Sekunden die CPU-Auslastung anzeigen lassen, aufgeschlüsselt nach den Kategorien *%user*, *%nice*, *%system*, *%iowait*, *%steal* und *%idle*. Der Wert von *%steal* ist nur bei virtuellen Maschinen von Bedeutung: Er zeigt an, wie viel Zeit der Prozessor mit der Ausführung anderer VMs verbracht hat. Weitere Felder – etwa *%irq* und *%soft* für die Bearbeitungszeit von Hard- und Software-Interrupts – lassen sich mit der Option *–u ALL* anzeigen.

Frei nach Heisenberg beeinflusst der beobachtende Prozess natürlich das Resultat. Jedoch nur geringfügig: auf dem Linux-PC des Autors etwa beansprucht *sar 10* lediglich wenige Sekunden Rechenzeit pro Tag. Wer nur eine Momentaufnahme benötigt, kann die Zahl der anzuzeigenden Datensätze als zusätzliches Argument übergeben: *sar 60 5* etwa zeigt fünf Minuten lang jede Minute die aktuelle CPU-Auslastung sowie am Ende einen Durchschnittswert an. Verfügt der Rechner über mehrere Prozessoren, beschränkt *–P <nummer>* die Ausgabe auf einen bestimmten; *–P ALL* zeigt die Last für jede CPU separat an.

Mit weiteren Optionen lässt sich der Fokus der Beobachtung verschieben. *sar –b* etwa zeigt Lese- und Schreibzugriffe auf den Massenspeicher an. Mit der Option *–d* schlüsselt *sar* die Daten obendrein nach Geräten auf. Wer sich für die Speicherauslastung interessiert, bekommt mit *–r* und *–S* die Belegung von Hauptspeicher und Swap-Bereich angezeigt. Die Optionen *–R*, *–B* und *–W* liefern statistische Daten zu Speicherallozierung, Paging und Swapping.

Daten über die Nutzung des Netzes lassen sich mit *sar –n <detail>* erfragen. Je nach Argument erhält der Nutzer die Transfer- oder Fehlerstatistik (*DEV* und *EDEV*), Informationen über die im Kernel integrierten NFS-Clients und -Server (*NFS* und *NFSD*), aktive Sockets (*SOCK*) sowie die komplette Statistik (*ALL*).

Daneben gestattet *sar* einen Blick auf die Ressourcen des Betriebssystems: *sar –v* zeigt die Zahl der genutzten Dateien, Inodes und Pseudo-Terminals (PTYs) an, *sar –w* die der erzeugten Tasks und Context Switches, *sar –q* die Zahl der gesamten und aktiven Tasks sowie die Systemlast.

Lässt man sich mehrere Kategorien anzeigen, gerät die Ausgabe schnell unübersichtlich. Wer mehrere Aspekte der Systemlast gleichzeitig beobachten will, tut das besser mit unterschiedlichen Kommandos in mehreren Fenstern. Greift der Admin zum Beispiel per Secure Shell *ssh* von außen auf den Rechner zu, kann er auch *screen* verwenden, um die Zahl der offenen Verbindungen zu reduzieren – muss allerdings zwischen den virtuellen Terminal-Fenstern hin und her blättern.

Onlinequellen

sysstat
pagesperso-orange.fr/sebastien.godard/

screen
www.gnu.org/software/screen/

Reise durch die Zeit

Eleganter ist es, Datenerfassung und -auswertung zu trennen. Für den Zweck existiert der separate System Activity Data Collector *sadc*, der üblicherweise abseits des normalen Suchpfads im Verzeichnis */usr/lib/sa* zu finden ist. Startet der Superuser ihn beim Booten mit */usr/lib/sa/sadc 60 <dateiname> &*, sammelt er im Minutentakt Daten ein und schreibt sie in einem kompakten binären Format auf die Festplatte, wo *sar* sie mit der Option *–f <dateiname>* abholen kann. Aus Platzgründen lässt *sadc* Informationen zu Interrupts und Plattenaktivität außen vor. Wer sie benötigt, kann sie mit *–S INT*, *–S DISK* oder *–S ALL* explizit anfordern.

Verwendet der Administrator als Dateinamen ein Minuszeichen, legt *sadc* jeden Tag unter dem Namen */var/log/sa/sa<dd>* eine frische Datei an. Die zwei Ziffern *<dd>* stehen für den jeweiligen Tag des Monats. Ältere, nicht mehr benötigte Dateien muss der Admin von Hand oder per Cron-Job verschieben, komprimieren oder löschen.

Analog verwendet *sar –f* – die Datensammlung des jeweiligen Kalendertages als Quelle. Benötigt der Nutzer die Daten eines anderen Tages, muss er den Dateinamen explizit angeben.

Ein dauerhaft laufender *sadc* belastet das System nur minimal. Sofern man ihn nicht gerade im Sekundentakt arbeiten lässt, hält sich auch das Datenvolumen in Grenzen – bei minütlicher Datenerhebung etwa 2 bis 3 MByte pro Tag. Es kann daher nicht schaden, den Data Collector beim Booten auf Verdacht zu starten. (mr)





Gewürze: Historie, Rezepte, Wirkung

Scharfe Sache

Diane Sieger

Ob Steakliebhaber oder Veganer – ohne Gewürze kocht keiner. Dass Kräuter und Knollen nicht nur den Geschmack von Speisen und Getränken beeinflussen, sondern auch Auswirkungen auf das körperliche und seelische Wohlbefinden haben, weiß vielleicht nicht jeder.



Schon seit Urzeiten verwendet der Mensch Gewürze, um den Geschmack seiner Nahrung zu verfeinern. Bereits in neolithischen Gräbern und Höhlen hat man würzende Kräuter und Sämereien gefunden, ebenso bei Ausgrabungen in Asien und insbesondere im Orient, der noch heute für seine leuchtend bunten, scharfen Gewürze berühmt ist.

Eine gute Ausgangsbasis für die Gewürzsuche im Internet bietet www.gewuerzindustrie.de/gewuerzkunde/gewuerzegeschichte.htm, denn hier erfährt der Leser alles rund um die Geschichte der Aromaspender. Beispielsweise ist von den erwähnten Ausgrabungen zu lesen, von der Entwicklung des Im- und Exports von Gewürzwaren im frühzeitlichen Handel sowie von der Bedeutung Alexandrias und Lissabons im Gewürzhandel.

Im späten 15. Jahrhundert haben portugiesische Entdecker die sogenannte „Gewürzroute“, also den Seeweg zwischen Europa und Indien, erschlossen. Von dieser Zeit an konnten auch die Europäer Pfeffer, Nelken, Muskatnuss und Zimt verwenden. Ausführliche Informationen zur Gewürzroute liefert Wikipedia (de.wikipedia.org/wiki/Gew%C3%BCrzroute). Dieser Beitrag geht ebenfalls ein wenig auf die Historie des Gewürzhandels ein.

Auch in der Literatur finden Gewürze früh Erwähnung. Schon Tafeln, die Archäologen bei Ausgrabungen im alten Babylonien entdeckten, enthielten Hinweise auf Gewürze; und selbst die Bibel erwähnt wohlriechende Gewürzmittel oft. Die Erzählungen aus Tausendundeiner Nacht, in der Kaufleute die Erlebnisse ihrer Handelsreisen schildern, dürfte vielen hinreichend bekannt sein. Nachzulesen ist all dies unter www.naturladen.ch/gewuerzegeschichte.htm#Gewürze%20in%20der%20Literatur.

Gewürz ist nicht gleich Mischung

Jeder kann mit Sicherheit spontan einige Gewürze aufzählen – Pfeffer, Chili und Muskat beispielsweise. Wer aber kann sagen, was ein Gewürz überhaupt ausmacht. Der Fachverband der Gewürzindustrie e. V., ein Zusammenschluss von rund 70 Gewürzverarbeitern und -veredlern, hat da eine Antwort parat. Unter www.gewuerzindustrie.de/leitsaetze/beschaffenheit1.htm hält der Verband genauestens fest, was ein Gewürz überhaupt ist und wie sich Gewürzmischungen, -präparate und -aromazubereitungen davon abgrenzen.

Wer an Details zu einzelnen Gewürzen interessiert ist, sollte sich auf Gernot Katzers Gewürzseiten (www.uni-graz.at/~katzer/germ/) umschauen. Auf seiner Website beleuchtet er 117 Gewürzpflanzen von Ajowan bis Zwiebel, inklusive Pflanzennamen in unzähligen Sprachen, sämtlichen Inhaltsstoffen und zahlreichen Fotos lebender Pflanzen und getrocknetem Gewürz. Weiterhin liefert der Autor zu jedem Gewürz eine umfangreiche Linkliste zu weiterführenden Informationen und Kochrezepten. Doch Vorsicht: Wenn man einmal anfängt, sich mit der Website zu befassen, wird es schwer, wieder loszulassen.

Wer nun einige der noch unbekannten Gewürze in der Küche verwenden möchte, sollte einen Blick auf das Webangebot des Gewürzherstellers Ostmann werfen. Unter www.gewuerze.de einfach zur Rezeptdatenbank durchklicken. Regelmäßig vorbeizuschauen lohnt sich insofern, als wöchentlich sieben neue Rezepte eingestellt werden.

Gewürze dienen jedoch nicht nur der Geschmacksverbesserung von Speisen. Auch wenn der Liebe ein wenig auf die Sprünge geholfen werden soll, kann man ins Gewürzregal greifen. Denn einige Gewürze wirken durchaus als Aphrodisiaka, unter anderem Muskat, Vanille und Chili. Genaueres zu diesem Thema weiß BerlinOnline.de unter www.berlinonline.de/themen/gesundheit-und-fitness/essen-und-geniessen/aphrodisiaka/index.php?page=1 zu berichten.

Vanille peppt Cola auf

Eins der bekanntesten und besonders unter Kuchenbäckern und Puddingschleckern beliebten Gewürze ist Vanille (www.ernestopauli.ch/Essen/Gew%C3%BCrze/Vanille.htm). Der Vanillegeschmack erfreut sich weltweiter Beliebtheit, sodass Softdrink-Riese Coca Cola das Gewürz kurzerhand seinem Verkaufsschlager hinzufügte. Noch heute ist Vanilla Coke in vielen Ländern dieser Erde erhältlich – ein witziger Werbespot aus dem asiatischen Raum ist unter www.youtube.com/watch?v=zi_8-dx0aew zu sehen.

Wer’s nicht vanillig, sondern lieber scharf mag, findet Gleichgesinnte im Chiliforum (www.chiliforum.net), denn hier lassen sich herrlich Tipps und Tricks rund um die Chili-Schote austauschen. Neben interessanten Erfahrungsberichten zu einzelnen Chili-Sorten gibt es unter anderem ausführliche Informationen zum Eigenanbau – die richtige Adresse für den Chili-Fan. Und letztendlich diskutiert man hier gern über Bhut Jolokia, die schärfste derzeit bekannte Chili-Sorte. Die Schärfe eines Lebensmittels bestimmt der Scoville-Wert, der Verdünnungsgrad, bei dem keine Schärfe mehr festzustellen ist. Dieser liegt bei Bhut Jolokia bei etwa ei-

ner Million. Nur wenige Menschen sind überhaupt noch in der Lage, eine derart scharfe Schote zu essen. Um Unterschiede zwischen verschiedenen Arten der schärfsten aller Schoten herauszufinden, hat pepperworld.com mit dem Eigenanbau experimentiert. Das Ergebnis gibt es unter www.pepperworld.com/botanisch/jolokia_vergleich.htm.

Natürlich kann man Gewürze nicht nur küchenfertig im Supermarkt erstehen. Die erste Adresse für besondere Produkte ist der Gewürz-Souk im Stadtteil Deira in Dubai. Dort gibt es alle nur erdenklichen Gewürze und zwar nicht nur im Glas oder in der Pappschachtel, sondern ganz frisch direkt aus dem Leinensack. Selbst wenn man nicht am Kauf der aromatischen Ware interessiert ist, lohnt sich ein Abstecher auf den basarähnlichen Markt, denn allein das Erschnuppern der außergewöhnlichen Gerüche und das Aufsaugen der Atmosphäre sind unbeschreiblich. Einen visuellen Vorgeschmack bieten einige Fotos aus dem Flickr-Set der Norwegerin Grete Howard (flickr.com/photos/11683866@N06/sets/72157606498658338/).

Wem Dubai zu weit ist, der kann sich auch in Hamburg umschauen. Die Speicherstadt in der Hansestadt ist der größte auf Eichenpfählen gegründete Lagerhauskomplex der Welt und steht seit 1991 unter Denkmalschutz. Früher kamen hier auf dem Wasserweg importierte Güter aus aller Herren Länder an, unter anderem Gewürze aus dem Orient. Die Geschichte des Gewürzhandels in Hamburg erzählt das private Gewürzmuseum Spicy's (www.spicys.de), das auf einem alten Lagerboden der Speicherstadt zu finden ist. Außerdem finden dort regelmäßig Veranstaltungen rund um das Thema statt, zum Beispiel Seminare mit Kochbuchautoren oder Lesungen mit Suppenausgabe – es lohnt sich also, den Veranstaltungskalender im Auge zu behalten.

Zum Schluss der definitive Beweis, dass Gewürze nicht nur in die Küche gehören: die „Spontane Gewürz Illumination". Youtube zeigt, was ein Künstler mit einem kleinen Haufen getrocknetem Oregano so alles anzufangen weiß (www.youtube.com/watch?v=9jE3naLCLvE). (ka)

URLs auf einen Blick

www.gewuerzindustrie.de/gewuerzkunde/gewuerzegeschichte.htm
de.wikipedia.org/wiki/Gew%C3%BCrzroute
www.naturladen.ch/gewuerzegeschichte.htm#Gewürze%20in%20der%20Literatur
www.gewuerzindustrie.de/leitsaetze/beschaffenheit1.htm
www.uni-graz.at/~katzer/germ/
www.gewuerze.de
www.berlinonline.de/themen/gesundheit-und-fitness/essen-und-geniessen/aphrodisiaka/index.php?page=1
www.ernestopauli.ch/Essen/Gew%C3%BCrze/Vanille.htm
www.youtube.com/watch?v=zi_8-dx0aew
www.chiliforum.net
www.pepperworld.com/botanisch/jolokia_vergleich.htm
flickr.com/photos/11683866@N06/sets/72157606498658338/
www.spicys.de
www.youtube.com/watch?v=9jE3naLCLvE

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/09/149/) hinzuzufügen.

Vor 10 Jahren: Die SmartCards, die Peripherie und die Zukunft

Das Schwerpunktthema der *iX* 9/1998 beschäftigte sich mit SmartCards, jenen Mikroprozessorkarten, die zum neuen Standard in der Computerperipherie gehören, wie man damals meinte.

Die Artikel thematisierten Java auf SmartCards und kluge Lesegeräte, die bald die Nutzung der Karten in jedem Desktop, PC oder an sonst einem Terminal möglich machen sollten. Diskutiert wurden Vor- und Nachteile kontaktloser und -behafteter SmartCards, und besonders ausführlich wurden die denkbaren Angriffsszenarien auf die Datenträger der Zukunft vorgestellt.

Heute wissen wir, dass USB-Sticks als Datenspeicher das Rennen gemacht haben und USB-Ports, die vor 10 Jahren nur an den besseren Notebooks zu finden waren, allgegenwärtig sind. In vielen anderen Bereichen dagegen sind SmartCards nach wie vor gefragt. Ihre Bedeutung wird in Zukunft noch zunehmen: Beim elektronischen Einkommensnachweis (ELENA) sollen Karten mit qualifizierter digitaler Signatur das Einverständnis des Arbeitnehmers dokumentieren, dass Finanzämter und Arbeitsagentur seine Einkommensdaten einsehen. Der elektronische Personalausweis soll als kontaktlose SmartCard ausgeliefert werden und Internet-Geschäfte absichern. Schließlich ist da die elektronische Gesundheitskarte (eGK), deren „Rollout" für Anfang 2009 geplant ist. Diese kontaktbehaftete Karte ersetzt die bisherige Krankenversichertenkarte (KSK) und ist Kernstück des weltgrößten PKI-Projekts.

Unter dem Titel „Kluge Medizin" findet sich in der *iX* 9/1998 eine erste Beschreibung des Systems, das die SmartCard des Patienten zusammen mit der Health Professional Card des Arztes in einer telematischen Infrastruktur einsetzt. Auch die heute diskutierten Anwendungsgebiete wurden vorgestellt: Notfalldaten, Medikationsgeschichte, Patientenakte und das elektronische Rezept samt besserer Liquidation ärztlicher Leistungen. *iX* zog das Fazit, dass der Patient mit „seiner einfach gestrickten Krankenversichertenkarte etwas unterversorgt ist". Bald würde eine kluge Karte die kluge Medizin beflügeln.

Zunächst unterscheidet sich die neue Gesundheitskarte, die über 80 Millionen Versicherte erhalten werden, technisch nicht von der KSK. Mit ihr können die Versichertendaten auf neu anzuschaffenden Lesegeräten ausgelesen werden, für weitergehende Anwendungen ist die Karte nur „vorbereitet". Nicht einmal die zentrale PKI-Funktion, mit der Patient und Arzt sich gegenseitig mittels der Telematik-Infrastruktur online authentifizieren, wird scharf geschaltet sein, weil die Testreihen der eGK noch gar nicht begonnen haben. Solange wird das elektronische Rezept – die „Pflichtanwendung" – ebenfalls nicht realisierbar sein. Damit greifen auch die Einsparungen nicht, die mit der Karte kommen sollen.

Dass die Gesundheitskarte überhaupt eingeführt wird, ist dem Wahlkampf geschuldet, der das komplizierte deutsche Gesundheitswesen auf einen griffigen Nenner bringen soll. So feiert die Politik das „Leuchtturmprojekt" der elektronischen Gesundheitskarte als Erfolg, während die Idee den 10. Geburtstag zelebrieren kann. *Detlef Borchers*

MEHR KBYTES

Skriptsprachen

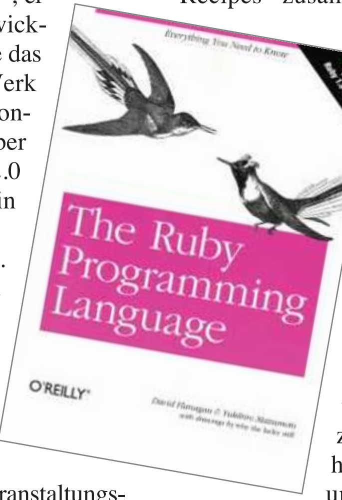
Spätestens seit dem nach seinen Erfindern Aho, Weinberger und Kernighan benannten *awk* (1977 entstanden) haben Skriptsprachen bei Programmierern einen festen Platz im „Herzen“. Zwar gibt es immer noch Menschen, die mit dem *awk* arbeiten (dieselben, die noch den *vi* als Editor nutzen :-), aber Sprachen wie Tcl haben ihren Höhepunkt lange hinter sich. Python wie Ruby dürften hingegen als richtige Erfolgsgeschichten gelten (Python liegt in Tiobes „Programming Community Index“ momentan vor Perl). Schon allein deshalb erscheinen Monat für Halbjahr weitere Bände zu diesen beiden Sprachen.

David Flanagan hat gemeinsam mit Matsumoto ein Handbuch für Ruby verfasst, das den älteren Matsumoto-Band der Nutshell-Reihe ersetzt und fortführt. „The Ruby Programming Language“ deckt nicht nur Version 1.8.x, sondern schon die kommende 1.9 mit ab. Als Grundlagenwerk mit fast kanonischem Charakter bekommt das Werk wohl bald einen festen Platz in vielen Regalen.

Spezieller hat Lyle Johnson sein bei den pragmatischen Programmierern erschienenes „FXRuby“ konzipiert. Es beschreibt, wie Entwickler mit der FOX-Bibliothek und dem darauf aufsetzenden FXRuby grafische Benutzerschnittstellen programmieren können – vom Einstieg mit „Hallo Welt“ bis zu fortgeschrittenen Techniken wie Menümanagement und Layout. Für Rubyisten, nicht für Rails-Anhänger.

Veröffentlichungen zu Ruby sind heutzutage allerdings meist solche, die das 2004 erstmals vorgestellte Web-Framework Ruby on Rails (oft Rails genannt) zum Inhalt haben. Hussein Morsy und Tanja Otto haben bei Galileo 700 Seiten samt einer DVD veröffentlicht, die gleichsam bei Null anfangen. Mit Herkunft, Installation und Ruby-Einführung haben Autor und Autorin die ersten 150 Seiten gefüllt. Und ab Seite 289 geht es ans Railsgemachte. Dabei orientieren sie sich ausdrücklich am Prinzip des Model View Controller (MVC), nach dem sie die Abschnitte gegliedert haben. Ajax hat ein eigenes Kapitel bekommen, das das in Rails entwickelte Prototype nutzt, und ein umfangreicher vierter Teil behandelt die Erweiterung von Rails durch Plug-ins, Sicherheitsaspekte und das Deployment. Schon durch seinen Umfang und Aufbau bietet der Band etwas für Fortgeschrittene.

Bettina Strackes „Web 2.0 mit Ruby on Rails“, erschienen bei entwickler.press, fußt wie das vorgenannte Werk auf Rails 2.0, konzentriert sich aber auf das Web 2.0 und soll kein Nachschlagewerk darstellen. Dementsprechend bespricht Stracke, was es mit dem Web 2.0 auf sich hat, bevor sie die Komponenten und Erscheinungsformen dieses Phänomens vorstellt: Ruby, Rails, Ajax, Mashups et cetera. Schließlich dient ein Veranstaltungskalender als Anwendungsbeispiel. Kapitel zu Ajax-Besonderheiten in Rails, der Integration von Karten und dem Deployment beschließen den Einsteiger-Band.



Nicht alle Autoren sprechen Anfänger an. Brad Edigers von O’Reilly veröffentlichtes „Advanced Rails“ setzt Kenntnisse in Ruby und Rails voraus, sein erstes Kapitel widmet er Meta- und funktionaler Programmierung. Des Weiteren handelt er Sicherheitsaspekte, Performancefragen, REST und Internationalisierung ab. Im Kapitel zu Datenbanksystemen diskutiert er etwa, welche DBMSe eine Alternative zu MySQL darstellen können und ob/wie Constraints, Trigger und Stored Procedures Platz in Rails-Anwendungen oder dem DBMS haben sollten.

Rezeptsammlungen können spannend sein. Mike Clark hat mit Unterstützung von über 50 Rails-Experten für die Pragmatic Programmers „Advanced Rails Recipes“ zusammengestellt, das nicht für den Einstieg gedacht ist. Ähnlich wie Ediger gliedert Clark nach Themen wie REST, Datenbanken, Benutzerschnittstelle, Performance und Sicherheit.

Andere Skriptsprachen haben ebenfalls ihre Reize, etwa das wie Ruby objektorientierte Python. Analog zum Galileo-Rails-Band haben Johannes Ernesti und Peter Kaiser ein „umfassendes Handbuch“ zu Python verfasst, dessen mehr als 800 Seiten zwar nicht für den mobilen Einsatz sprechen, aber als Lern- und Nachschlagewerk dienen können. Ähnliches gilt für Peter Walerowskis Grundlagenwerk zur selben Sprache, das Addison-Wesley verlegt hat. Mit gut 300 Seiten gerät die Einführung logischerweise etwas knapper und leichter transportierbar.

Beim objektorientierten Groovy handelt es sich um Python für Java-Programmierer. Das suggeriert zumindest Joachim Baumanns Einführung zu dieser Skriptsprache, die dpunkt in diesem Jahr veröffentlicht hat. Und bei den pragmatischen Programmierern gibt es auch zu Groovy Einführendes, wie immer auf Englisch und in diesem Fall von Venkat Subramaniam. Beide Bände haben den Charakter eines Lern- und Nachschlagewerks, Baumanns wegen des größeren Umfangs mit vielleicht noch mehr Details.

Henning Behme

Joachim Baumann; Groovy; Grundlagen und fortgeschrittene Techniken; Heidelberg (dpunkt) 2008; 587 Seiten; € 46,– (gebunden)

Mike Clark and the Rails Community; Advanced Rails Recipes; Raleigh, NC (Pragmatic Bookshelf) 2008; 447 Seiten; US-$ 38,95 (Paperback)

Brad Ediger; Advanced Rails; Sebastopol, CA (O’Reilly Media) 2007; 342 Seiten; € 34,– (Paperback)

Johannes Ernesti, Peter Kaiser; Python; Das umfassende Handbuch; Bonn (Galileo Press) 2008; 819 Seiten zzgl. CD-ROM; € 39,90 (gebunden)

David Flanagan, Yukihiro Matsumoto; The Ruby Programming Language; Sebastopol, CA (O’Reilly Media) 2008; 429 Seiten; € 38,– (Paperback)

Lyle Johnson; FXRuby; Create Lean and Mean GUIs with Ruby; Raleigh, NC (Pragmatic Bookshelf) 2008; 219 Seiten; € 36,95 (Paperback)

Hussein Morsy, Tanja Otto; Ruby on Rails 2; Das Entwickler-Handbuch; Bonn (Galileo Press) 2008; 699 Seiten; € 39,90 (gebunden)

Bettina Stracke; Web 2.0 mit Ruby on Rails; Professionelle Anwendungen mit Ajax, Mashups und dem Rails Framework; Unterhaching (entwickler.press) 2008; 299 Seiten; € 39,90 (gebunden)

Venkat Subramaniam; Programming Groovy; Dynamic Productivity for the Java Developer; Raleigh, NC (Pragmatic Bookshelf) 2008; 300 Seiten; US-$ 34,95 (Paperback)

Peter Walerowski; Python; Grundlagen und Praxis; München (Addison-Wesley) 2008; 318 Seiten zzgl. CD-ROM; € 29,95 (Paperback)



Mercedes Bunz

Vom Speicher zum Verteiler

Die Geschichte des Internet

Berlin 2008
Kulturverlag Kadmos
147 Seiten
17,50 €
ISBN 978-3-86599-025-9

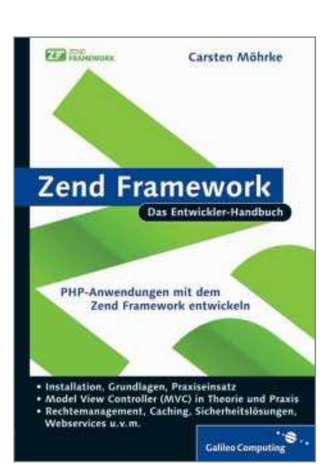
Laut Verlag verfolgt dieses Buch die Entstehung des Internet von den „frühen Planungen der ersten Netzwerke bis hin zum heutigen Internetprotokoll“. Das ist übertrieben: Begriffe wie „klassenloses Routing“ oder „Label Switching“, die für die Evolution des Internet entscheidend waren, kommen darin nicht vor. Geschichte heißt hier Frühgeschichte. Damit muss es sich den Vergleich mit Janet Abbates „Inventing the Internet“ (1999) gefallen lassen.

Wo Abbate die Entwicklung auf der Grundlage eines soliden Verständnisses der involvierten Probleme präzise darstellt, dominiert hier der sich in einer gespreizten Sprache äußernde Ehrgeiz, medientheoretischen Tiefsinn zu produzieren. Das fängt an mit der Unfähigkeit, Abstrakta korrekt zu verwenden oder zwischen Adjektiven und Adverbien zu unterscheiden, über banalen Schwulst bis hin zu gehobenem Nonsens (S. 62: „Store-and-Forward ist im verteilten Netzwerk also vor allem ein Prinzip, um die Sendung in Bewegung zu halten und auf diese Weise die Geschwindigkeit ihres Ankommens zu erhöhen“).

Während sich wenigstens ein paar historische Ereignisse wiederfinden, deren institutioneller Kontext jedoch unterbelichtet bleibt, gehen die technischen Zusammenhänge in dem medientheoretischen Gebräu vollends unter. Weshalb E-Mail eine Form der Eins-zu-eins-Kommunikation sein soll, bleibt angesichts millionenfachen Spams ein Geheimnis der Autorin. Und dass Filesharing-Netze die technische Struktur des Internet erst wirklich aufnähmen und ausnutzten, ist reine Fantasie: Weder entsprechen die Topologie und die Routing-Protokolle des Internet den in Paul Barans Rand-Memorandum entwickelten Konzepten des verteilten Netzes, noch hat die Verteilung von Dateien in einem Filesharing-Netz etwas mit der Topologie und den Routing-Protokollen des darunterliegenden Kommunikationsnetzes zu tun.

Die Suche nach einer durchgängigen Logik der Verteilung in der Geschichte des Internet artet so in Verbalfetischismus aus, der illusionäre Ansichten hervorbringt und Banalitäten als bahnbrechende Erkenntnisse ausgibt, wie dass Neuerungen selten nur an einem Ort entstehen. Eine Übersetzung von Abbates Buch wäre besser gewesen.

RAINER FISCHBACH



Carsten Möhrke

Zend Framework

Das Entwicklerhandbuch

Bonn 2008
Galileo Press
420 Seiten
39,90 €
ISBN 978-3-8362-1068-3

Seit einiger Zeit findet das Entwurfsmuster Model-View-Controller (MVC) zur Aufteilung von Softwaresystemen mehr und mehr Verbreitung in PHP (siehe CakePHP, CodeIgniter und Symfony). Es war daher nur eine Frage der Zeit, bis die PHP-Firma Zend ein eigenes Framework auf den Markt bringen würde, das sie mittlerweile als Version 1.5 zum Download anbietet. Carsten Möhrke hat mit dem vorliegenden Werk das erste Buch dazu in deutscher Sprache veröffentlicht.

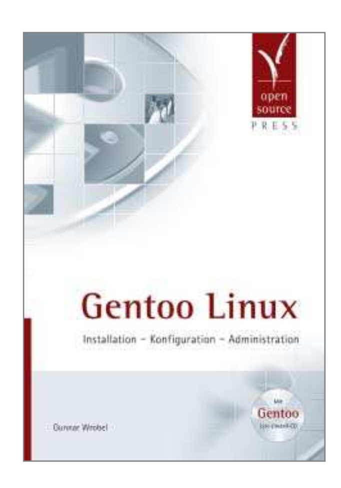
Besonderen Wert legte Möhrke darauf, dass jedes der acht Kapitel einzeln nachvollziehbar ist, ohne dass Leser auf die Beschreibung anderer Klassen zurückgreifen müssen. Damit erspart er ihnen unnötiges Hin- und Herblättern und verdeutlicht zudem die getrennte Nutzbarkeit unterschiedlicher Komponenten. Die Beschreibung der jeweiligen Klassen beschränkt er auf das Wesentliche – mit kurzen Codebeispielen. Dabei lässt der Autor zahlreiche für die tägliche Praxis durchaus hilfreiche Informationen einfließen, die in der offiziellen Dokumentation unerwähnt bleiben.

Im ersten Kapitel geht es um Theorie und Grundlagen des Framework. Das zweite zeigt, wie man auf Datenbanken zugreift; ein weiteres beschäftigt sich mit Benutzer- und Rechteverwaltung. Dazu bietet das Framework wahlweise ACL, HTTP oder Sessions an. Ein großes Kapitel widmet der Autor diversen Aufgaben, angefangen von Komponenten für die Cache-Kontrolle oder dem Prüfen und Filtern von Daten, bis hin zu fortgeschrittenen Themen wie dem Erzeugen von Logdateien, der Verwaltung von Konfigurationsdateien oder der Shell-Programmierung auf Basis des Framework.

Die zweite Hälfte startet mit Komponenten für den Zugriff auf Webservices. Dazu bietet Zend komfortable Klassen für die Arbeit mit Feeds im Allgemeinen (RSS, Atom) und den APIs von Amazon, Flickr, Yahoo oder Google. Kapitel sechs stellt Komponenten für die Arbeit mit E-Mail vor und zeigt unter anderem den Zugriff auf SMTP- und IMAP-Server. Anschließend werden die Klassen für das Bearbeiten von JSON-Daten und das Generieren von PDF-Dokumenten vorgestellt. Die letzten beiden Kapitel arbeiten mit Protokollen (HTTP, XML-RPC, REST) und der Lokalisierung von Daten. Die mitgelieferte CD-ROM enthält alle Listings sowie das PEAR-Buch des Autors als E-Book.

Aufgrund der komplexen Architektur des Framework kann der Band nicht alles im Detail beschreiben. Es ist dem Autor aber gelungen, alle relevanten Funktionen vorzustellen, sodass Anfänger und Fortgeschrittene sich schnell zurechtfinden. Leider konnte Version 1.5 nicht mehr berücksichtigt werden. Allerdings verspricht der Autor, in seinem Blog (zf-buch.de) aktuelle Kapitel als PDF-Versionen zum Download bereitzustellen. Ein gelungenes Buch für Einsteiger und Fortgeschrittene.

JOHANNES GAMPERL



Gunnar Wrobel

Gentoo Linux

Installation – Konfiguration – Administration

München 2008
Open Source Press
416 Seiten
39,90 €
ISBN 978-3-937514-34-5

Für fortgeschrittene Linux-Anwender, die sich ihre Systemumgebung flexibel zusammenstellen und dabei unabhängig von den üblichen Binär-Distributionen bleiben wollen, ist Gentoo-Linux das System der Wahl. Eine Gentoo-Installation besteht nicht aus vorkonfigurierten Binärpaketen, sondern wird auf dem eigenen PC vollständig aus den Quelltexten kompiliert. Diese werden beim Vorliegen neuer Programmversionen in kleinen, kontinuierlichen Schritten aktualisiert. So kommt es nicht zu den großen und manchmal schwierigen Release-Sprüngen, wie man sie von vielen Binärdistributionen her kennt.

Unterschiede zu anderen Linux-Systemen offenbart Gentoo nicht nur in seiner Philosophie, sondern auch in Installation und Wartung. Wrobels Buch führt auf der Basis der beiliegenden Gentoo-Live-DVD für x86-Rechner in die Werkzeuge und Besonderheiten des Systems ein. Der Leser, der schon Linux-Erfahrung mitbringen muss, lernt das System schrittweise kennen – von typischen Wartungsaufgaben bis hin zu speziellen Fragestellungen. Dabei konzentriert Wrobel sich auf die bei Gentoo üblichen Kommandozeilenwerkzeuge. Der noch in einem frühen Stadium befindliche grafische Installer kommt nur am Rande vor, aber Gentoo wird ohnehin überwiegend über die Kommandozeile administriert.

Die gebotenen Konfigurationsmöglichkeiten bespricht der Autor ausführlich hinsichtlich ihrer Wirkung und der damit verbundenen Vor- und Nachteile. Um den Überblick über wichtige Schalter zu wahren, fasst ein Kapitel die geläufigen Einstellungen zusammen. Weitere Themen sind Kernel- und Netzkonfiguration, Bootprozess, Lokalisierung und insbesondere das Paket- und Abhängigkeitsmanagement. Die beispielhafte Einrichtung eines Webservers demonstriert die praktische Anwendung der Kommandozeilenwerkzeuge. Wer nicht nur reiner Anwender der vom Gentoo-Projekt verwalteten Quelltext-Pakete bleiben will, sondern eigene definieren möchte, erhält in weiteren Kapiteln das Rüstzeug dazu.

Obwohl es zahlreiche Informationsquellen zu Gentoo-Systemen gibt, ist dem Autor, der sich offensichtlich intensiv mit Gentoo auseinandergesetzt hat, eine gut lesbare Darstellung mit eigenständigem Charakter gelungen.

UWE SEIMET



Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Urbanski, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Bianca Nagel (-456, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo⁺ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

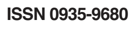
Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo*⁺ (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de

ISSN 0935-9680







Videokonferenzen per Telepräsenz

Wie an einem Tisch sollen die Konferenzteilnehmer sitzen, auch wenn sie über alle Erdteile verteilt sind. Bewerkstelligen sollen das Telepräsenz-Systeme, die moderne Audio- und Videotechnik mit einer ausgeklügelten Kombination aus Konferenztischgestaltung, Kamerapositionen und Raumdesign kombinieren. Eine Gegenüberstellung zweier Produkte dokumentiert zugleich den Stand der Technik.

Business-Reporting im Vergleich

Neben den klassischen Produkten haben sich im Business-Intelligence-Umfeld einige Open-Source-Anwendungen etabliert, die ihren kommerziellen Kollegen durchaus das Wasser reichen können. Je ein Protagonist aus der kostenpflichtigen und der freien Reporting-Welt, namentlich das Eclipse-Projekt BIRT und der Desktop-Marktführer Crystal Reports, zeigen ihre Stärken und Schwächen.

Refactoring gegen Erosion

Das Schicksal von Softwaresystemen ist, dass sie nie wirklich abgeschlossen sind. Neue Wünsche der Anwender und strukturelle Notwendigkeiten bedingen die kontinuierliche Erweiterung von Softwarearchitekturen. Ein unsystematisches Wachstum kann aber leicht zu Erosionsprozessen führen. Das probate Gegenmittel ist ein regelmäßiges architektonisches Refactoring.

Heft 10/2008 erscheint am 18. September 2008

Marktübersicht: PC-Management

Zum einen geht's um klassisches Client-Management mit Softwareverteilung, Inventarisierung, Fernsteuerung, Profilmanagement und zum anderen um Endpoint Security mit I/O- und Applikationskontrolle, erweitertes Patchmanagement, Schwachstellenanalyse, Daten- und Laufwerksverschlüsselung. Ein besonderes Augenmerk gilt dabei der Unterstützung der neuen Funktionen von Vista.

Bürgerkommunikation 2.0

Im Rahmen von „E-Government 2.0“, bekannt durch den jüngst beschlossenen elektronischen Personalausweis, möchte der Bund auch Rahmenbedingungen für eine „sichere und verbindliche elektronische Kommunikation“ durchsetzen. Sogenannte Bürgerportale und eine rechtssichere E-Mail-Alternative namens D-Mail sollen die Bürger trotz angeknacksten Vertrauens in das Internet zur elektronischen Abwicklung ihrer Pflichten ermutigen.



Das bringen





Netbooks: Aufs Wesentliche reduzierte Mini-Notebooks

Displays: Trends von Monitor bis TV

Mehrwert-Navis trumpfen mit Extras auf

Farbdrucker: Laser oder Tinte?

Heft 18/08 jetzt am Kiosk





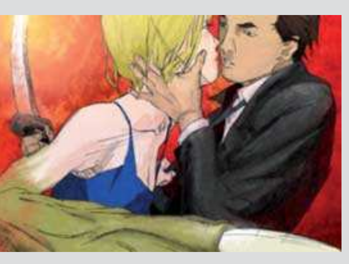
Automatisch günstige Stromtarife: Intelligente Stromzähler senken Kosten.

Wo sind sie? Weshalb die Entdeckung außerirdischen Lebens eine schlechte Nachricht wäre.

Leichtbau: Kampf um jedes Kilo

Heft 9/08 jetzt am Kiosk

TELEPOLIS
MAGAZIN DER NETZKULTUR



Marcus Hammerschmitt: Menschenfresser und Samurai – Die hohe Schule des Anime-Surrealismus: Monster-Sushi à la „Kemonozume“

Jörg Auf dem Hövel: Big Pharma sucht nach Orientierung

www.heise.de/tp/